Voice over IP: Risks, Threats, and Vulnerabilities

Angelos D. Keromytis
Network Security Lab
Columbia University
angelos@cs.columbia.edu

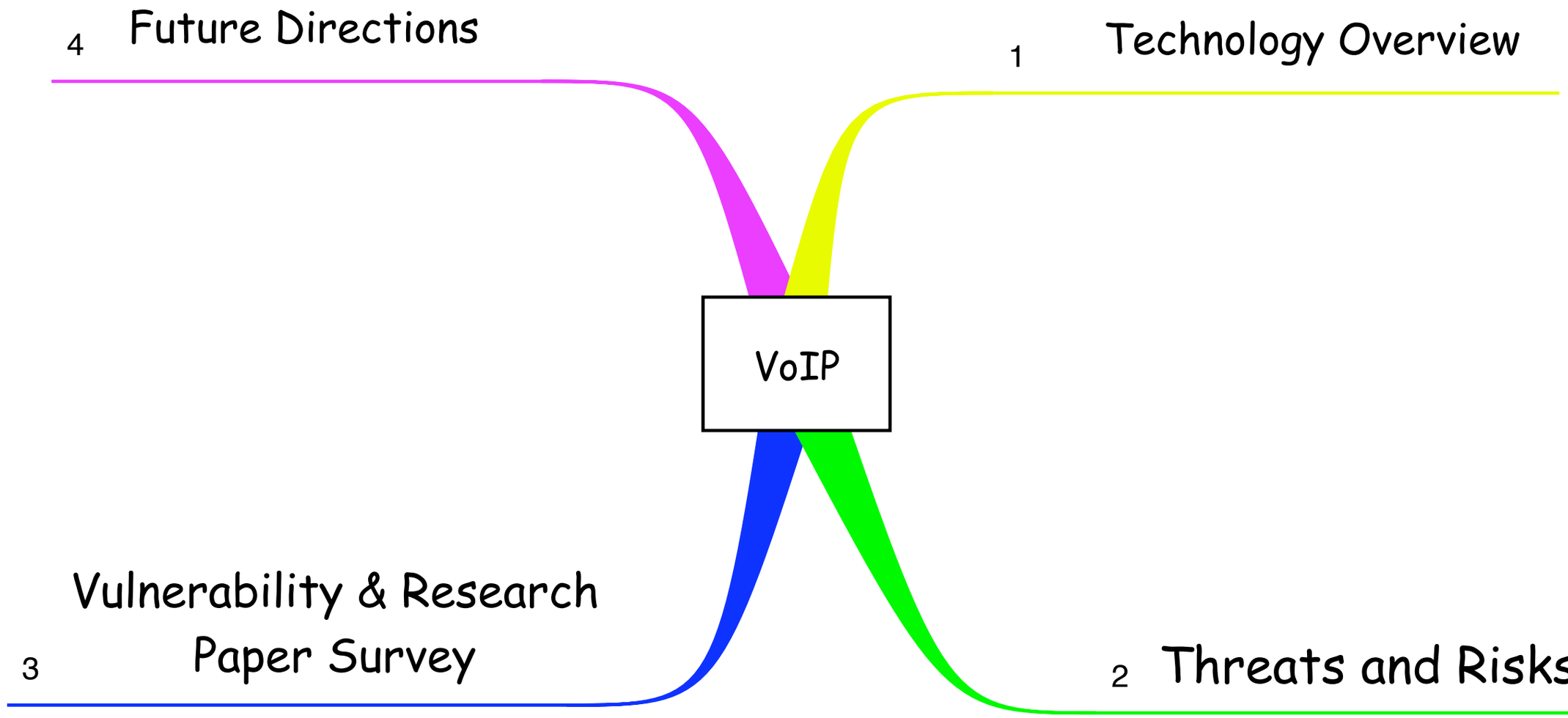
Why care about VoIP security?

- Increasing deployment and use
  - consumer, enterprise and government
- Highly complex system-of-systems
- Attractive target
  - carries sensitive data
  - provides critical services
  - immediate monetization

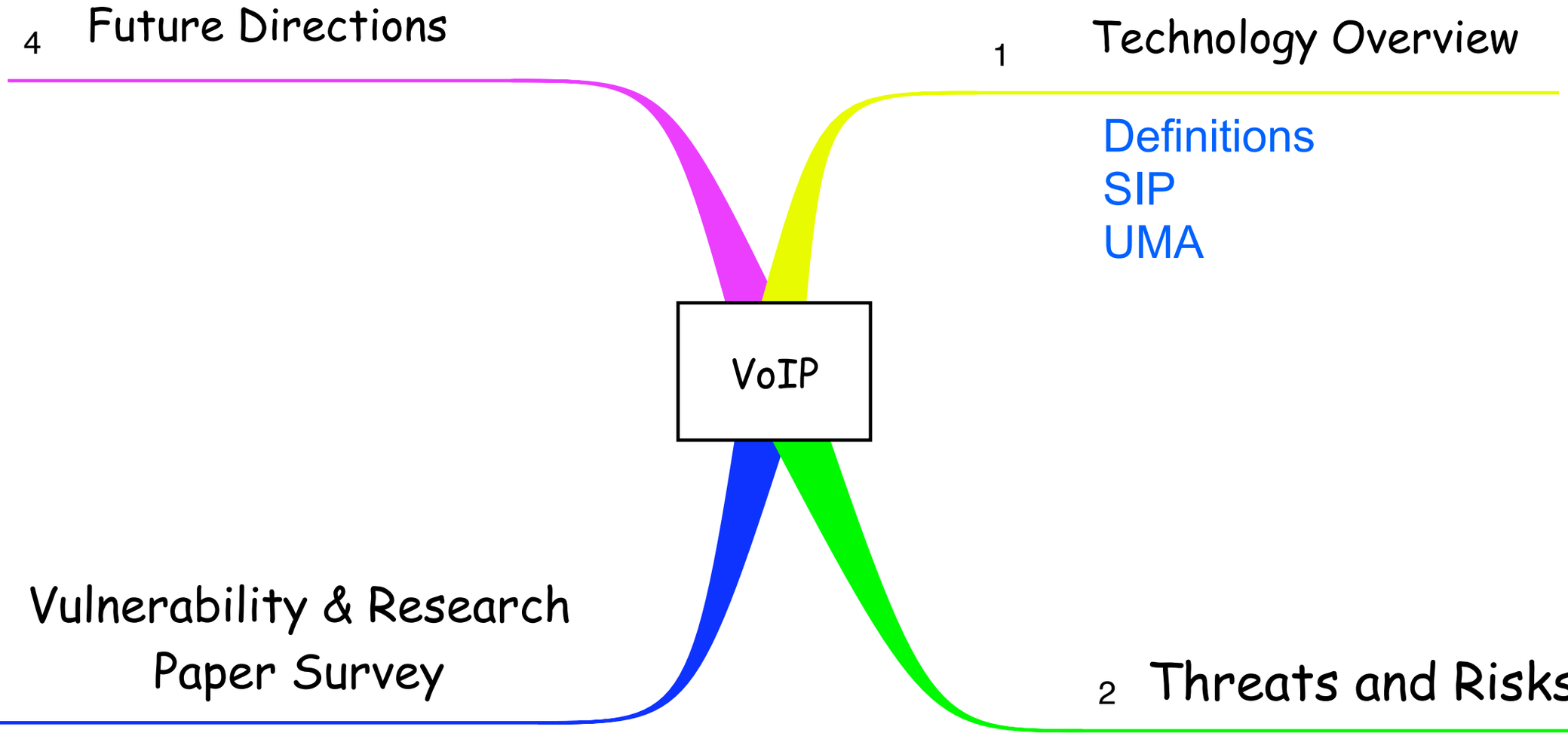
Why talk about it?

- Most research to date has focused on components
  - little to no “big picture” analysis of VoIP systems and infrastructures
  - emergent properties and nasty system interactions fall through the cracks
- Little understanding of how theoretical risks related to the real world
  - disconnect between what we worry about and what we are known to be vulnerable to
- Think about how we design future systems

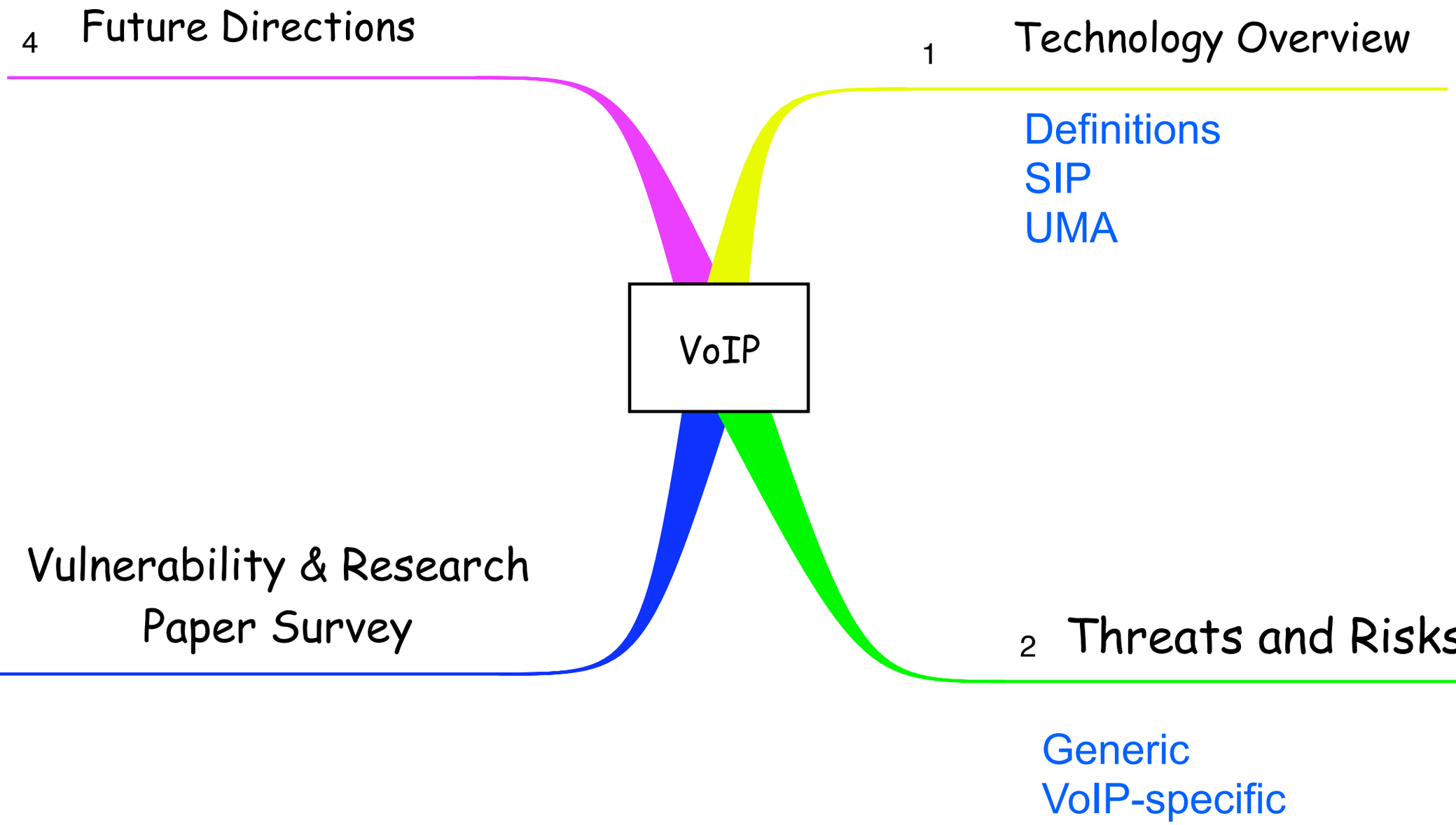
What this talk is about



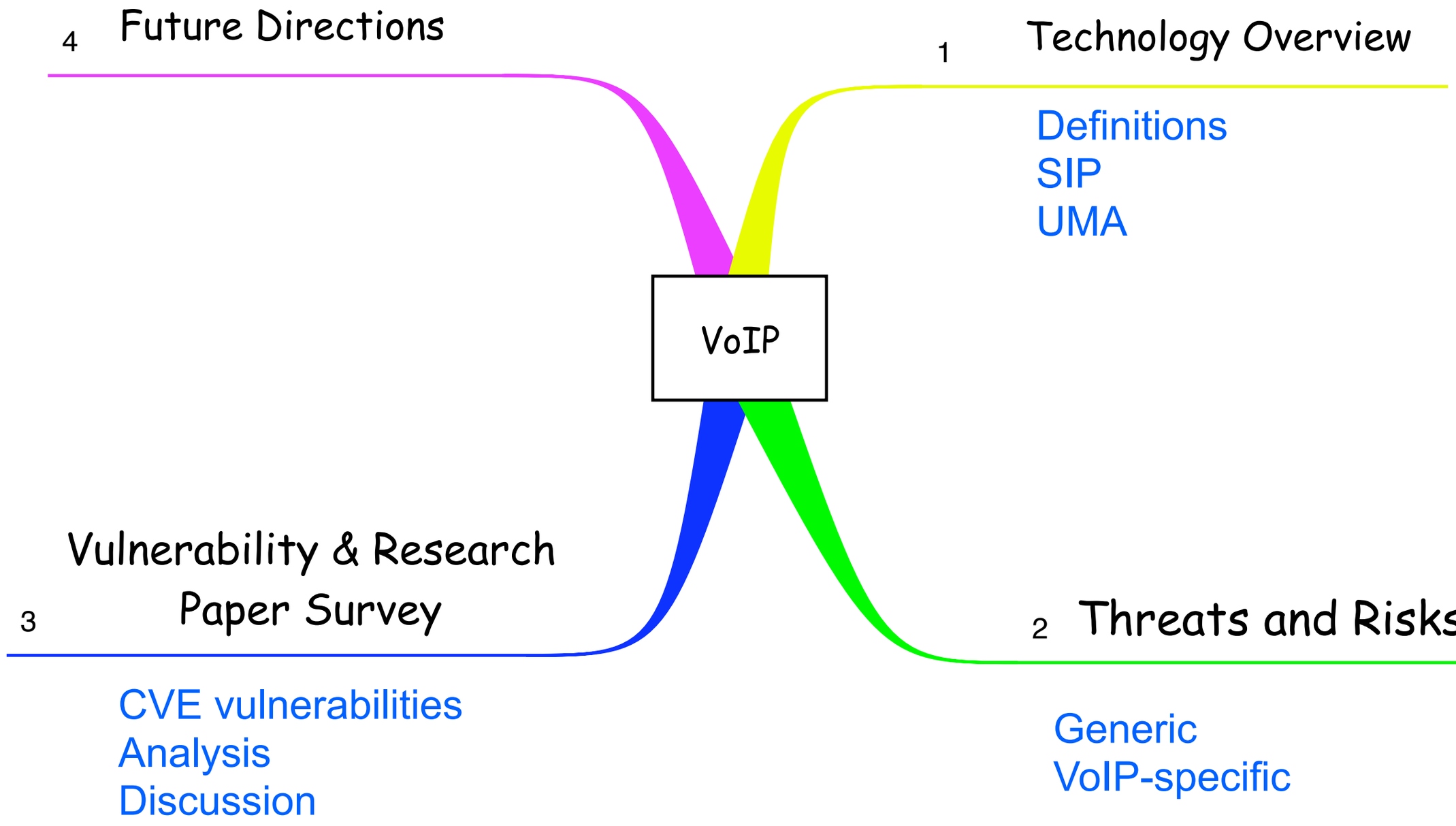
What this talk is about



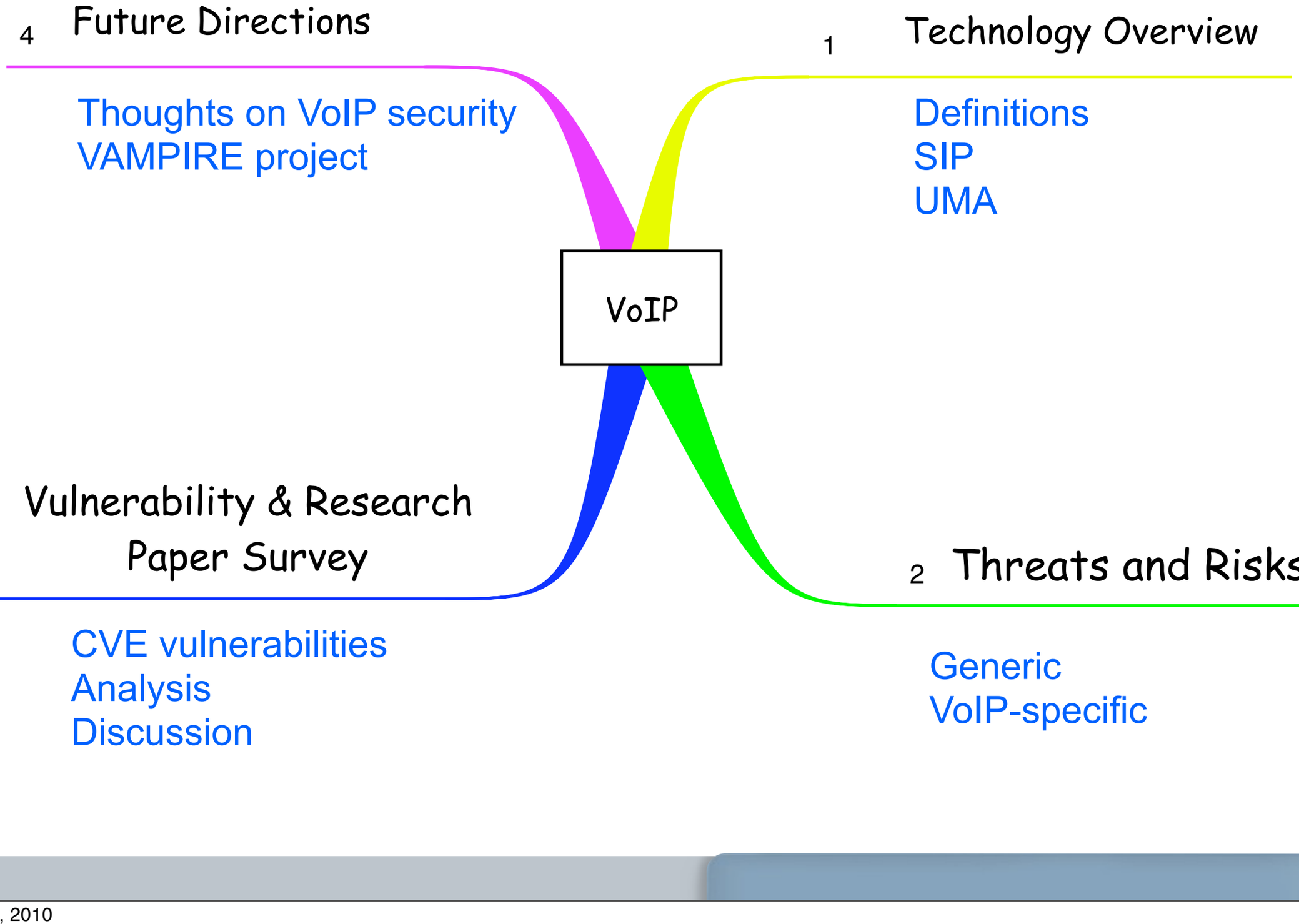
What this talk is about



What this talk is about



What this talk is about



What is VoIP/IMS?

- Protocol(s) for voice communication over IP-based infrastructures
  - use of the Internet itself is dependent on operator

- Voice over IP: catch-all term

- IP Multimedia Subsystem: industry standard for IP-based multimedia communications
  - video, calendaring/scheduling, file-sharing, collaborative editing, ...

VoIP in the marketplace

- Basis for many products/services
  - commercial: Vonage, 3, T-Mobile/UMA, T-Mobile@Home, ...
  - free/semi-free: Skype, GTalk, MSN, Yahoo! IM, AIM, Gizmo, ...
- Both enterprise- and consumer-oriented
  - management simplification
  - cost reduction
- Various architectural models
  - centralized vs. P2P
  - open vs. closed

Components

- Signaling
  - responsible for call setup and management
  - architectural and operational components
    - principal/endpoint naming
    - IP mapping
    - proxying
    - billing
    - access control
    - device configuration/management
    - customer support
    - QoS
- Data transport
  - codecs, transport protocols (typically RTP), QoS, content security

IMS protocols

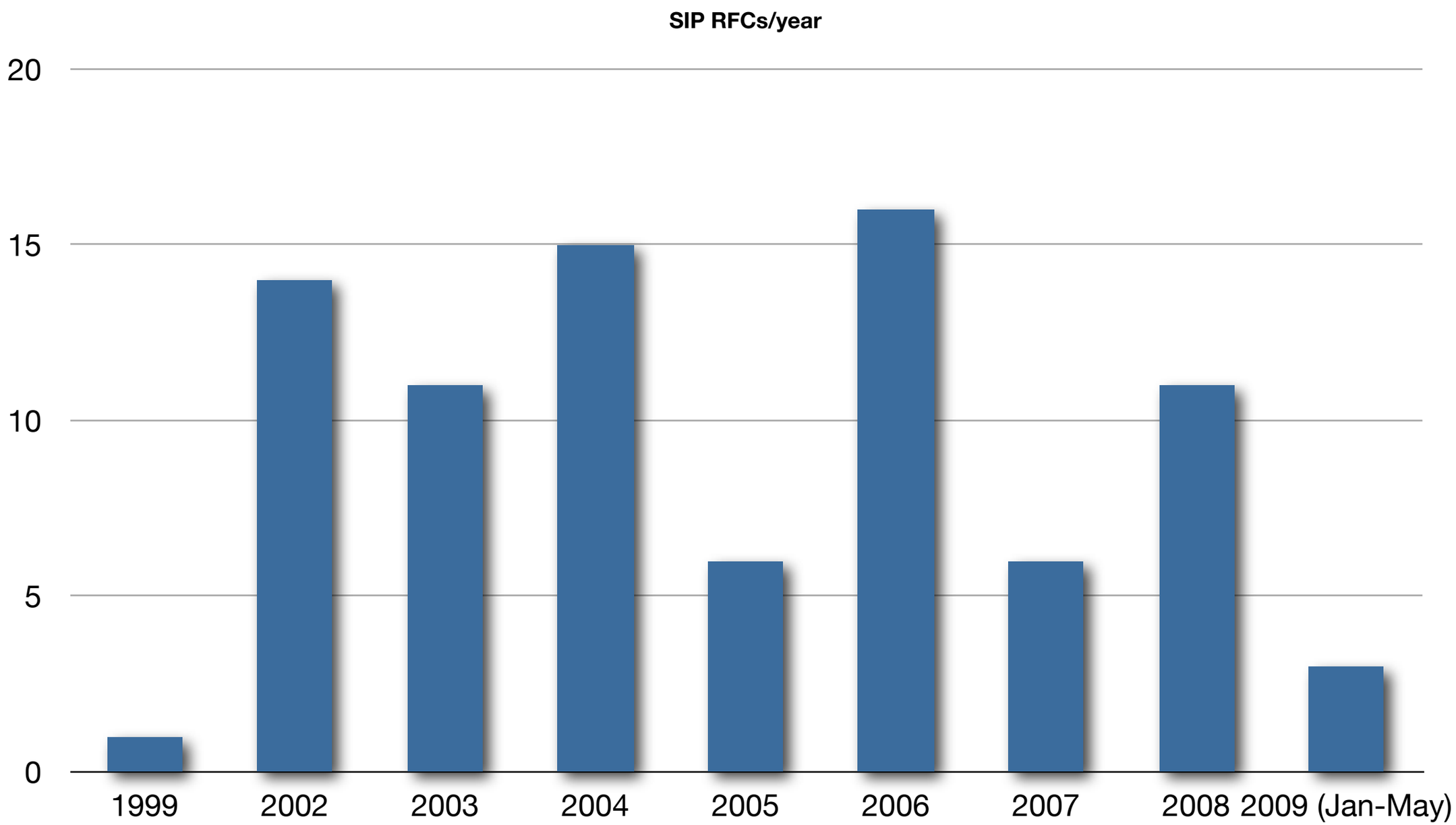
- Two predominant mechanisms
  - Session Initiation Protocol (SIP)
    - H.323 used in some environments
  - Unlicensed Mobile Access (UMA)

- Other popular mechanisms exist
  - Skype, Asterisk, GTalk/AIM ...

Session Initiation Protocol (SIP)

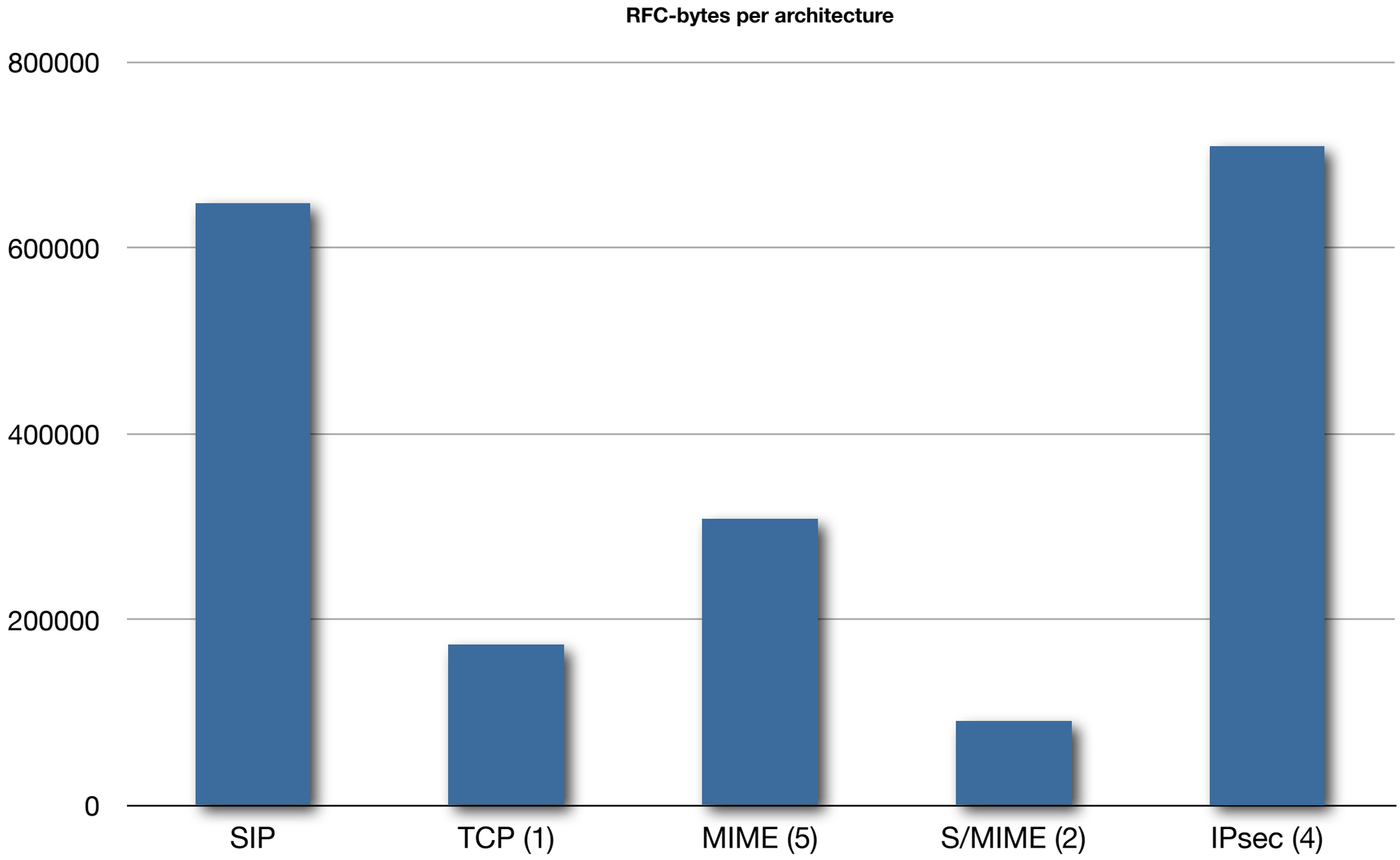
- Signaling protocol for IMS
  - similar to HTTP
    - text-based
    - request/response structure
    - uses HTTP Digest Authentication (adapted to SIP) for user authentication
  - unlike HTTP, it is stateful
    - highly complex FSM, source of numerous (most?) vulnerabilities

SIP complexity

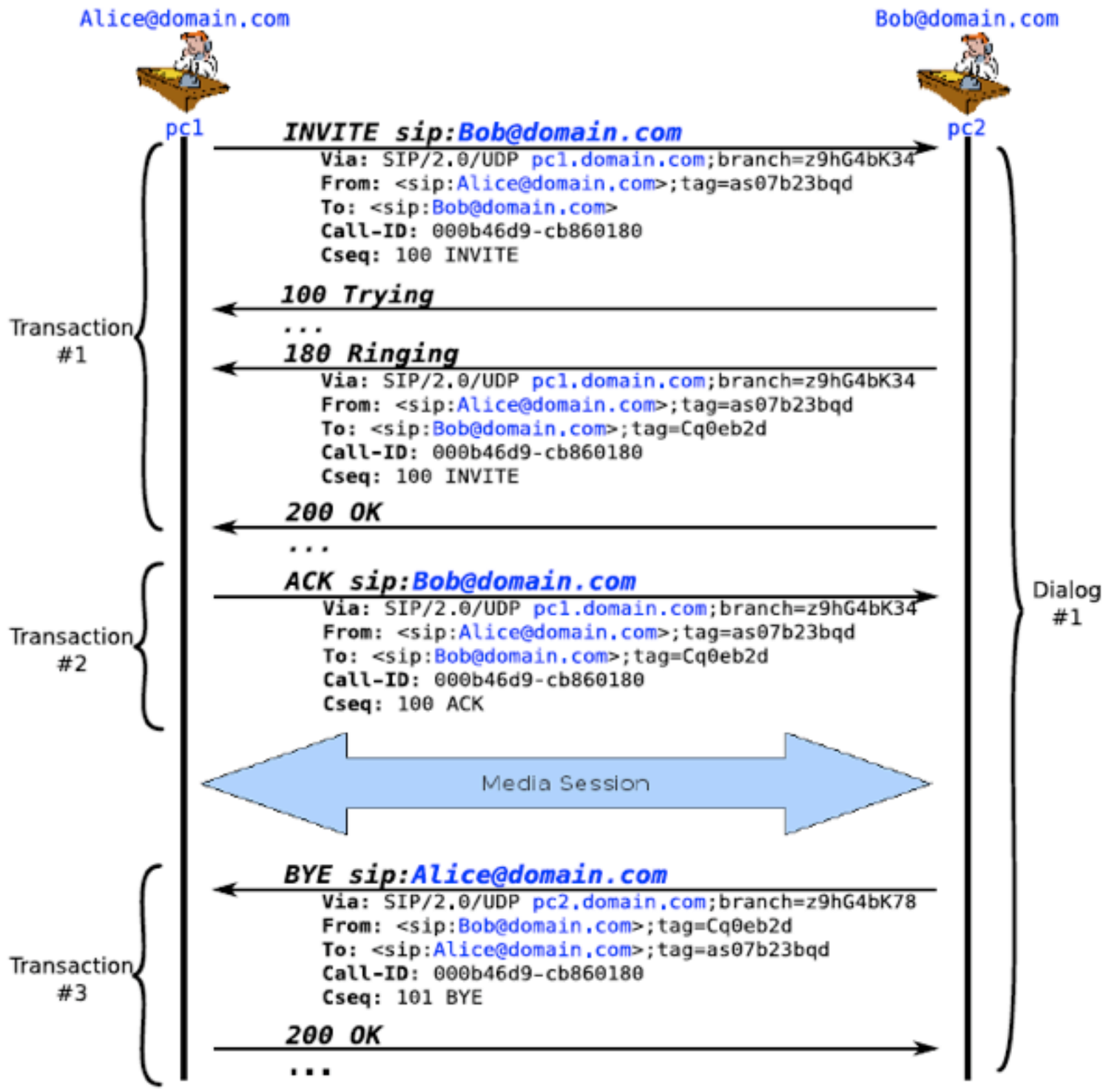


RFC 3261

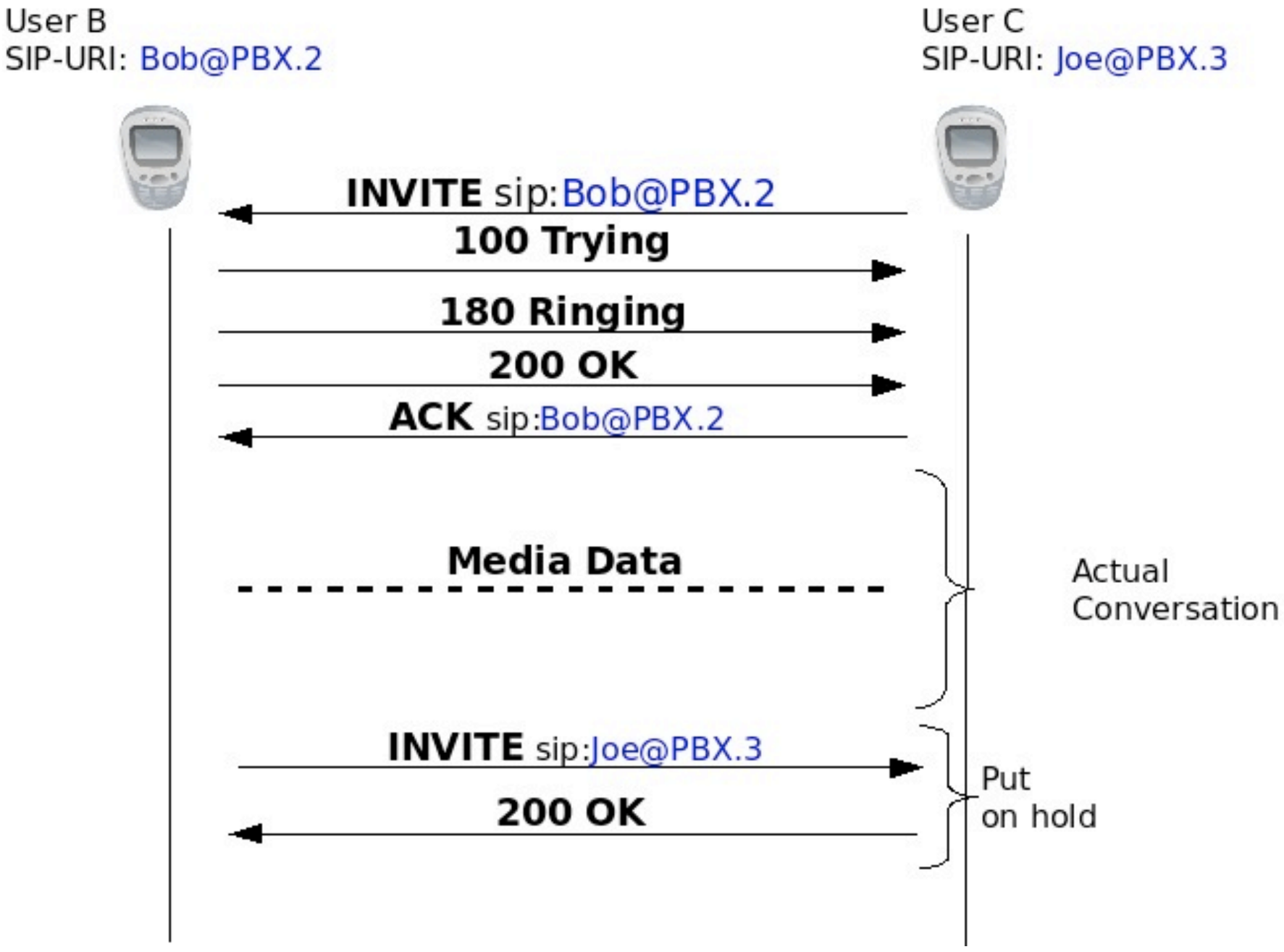
- Main SIP RFC is 2nd-largest ever (after “Internet Security Glossary”)



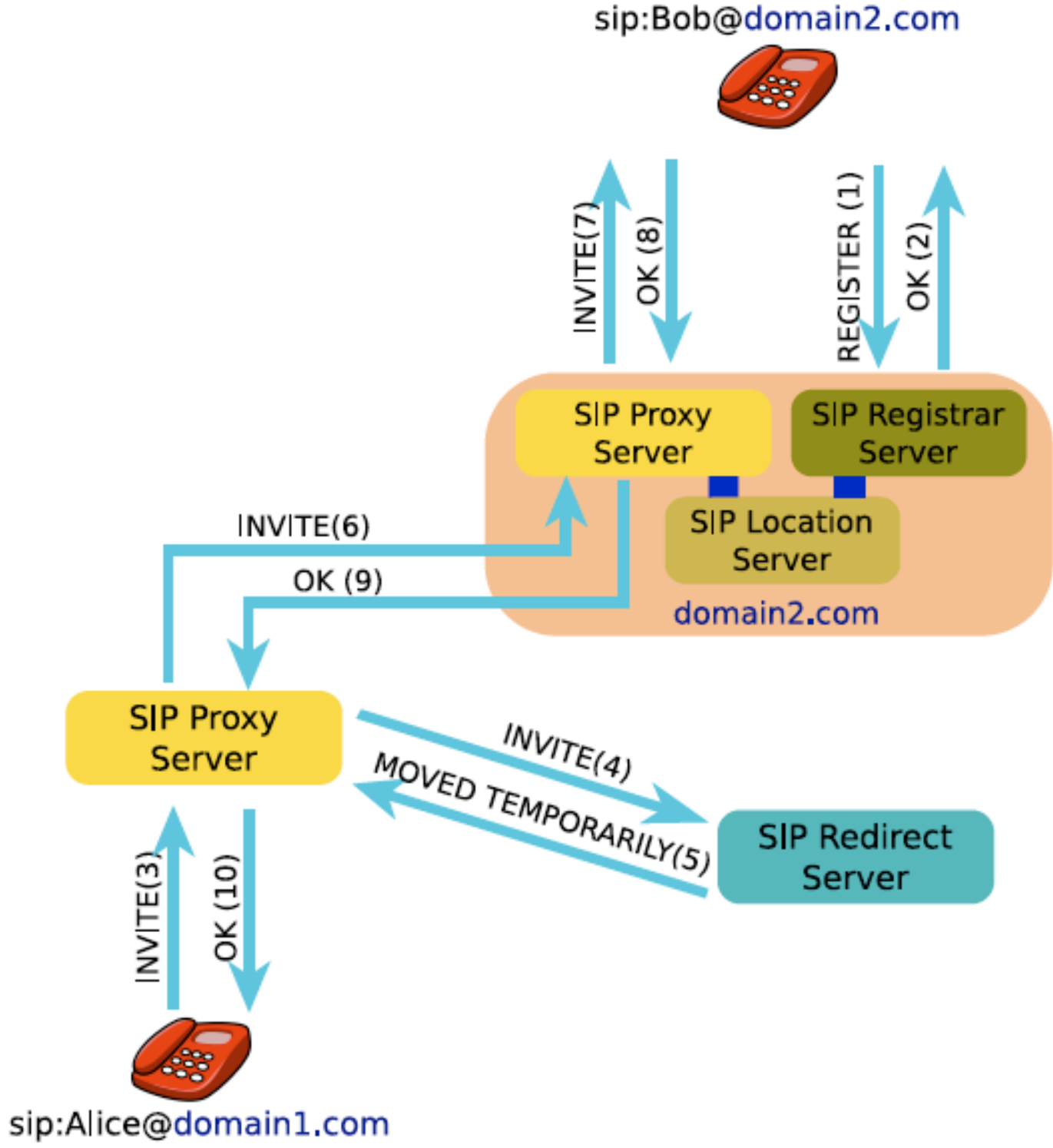
SIP exchange



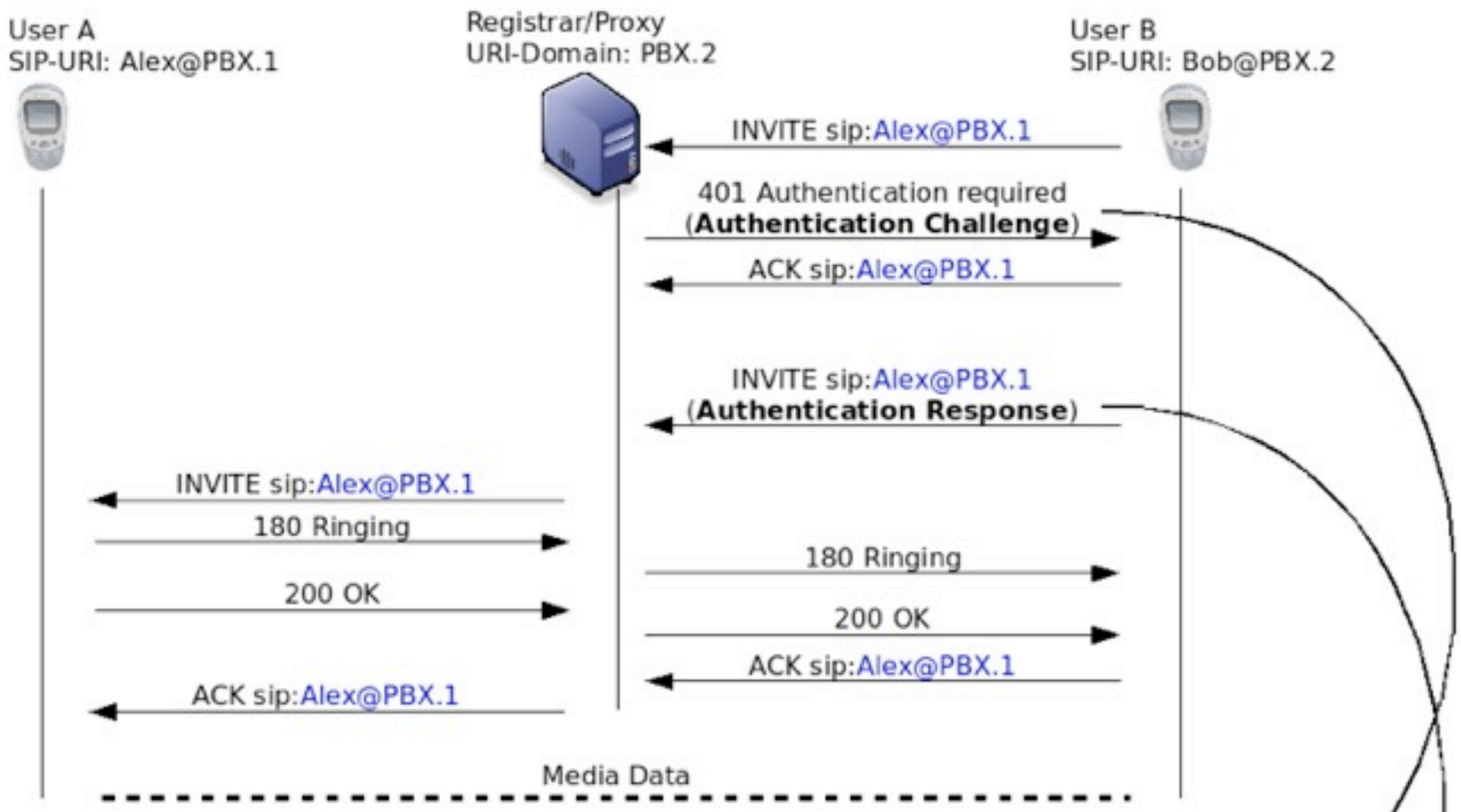
Call forwarding



SIP component interactions



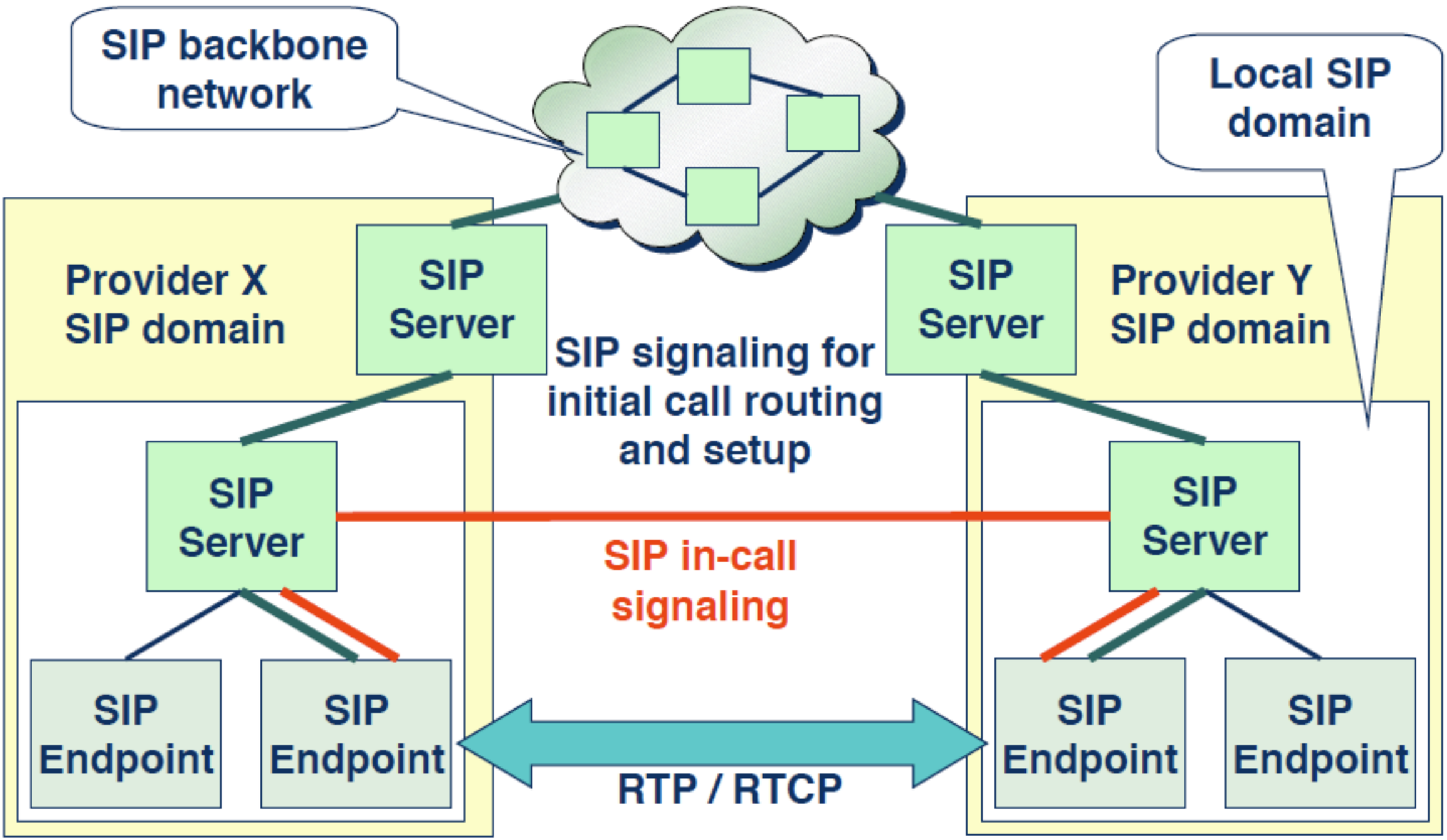
SIP authentication



Proxy-Authenticate: Digest algorithm=MD5,
realm="domain.org",
nonce="1d78fb72"

Proxy-Authorization: Digest username="Bob",
realm="domain.org",
uri="sip:Alex@PBX.1",
response="4cc8a1de5a60306c760",
nonce="1d78fb72", algorithm=MD5

SIP architecture



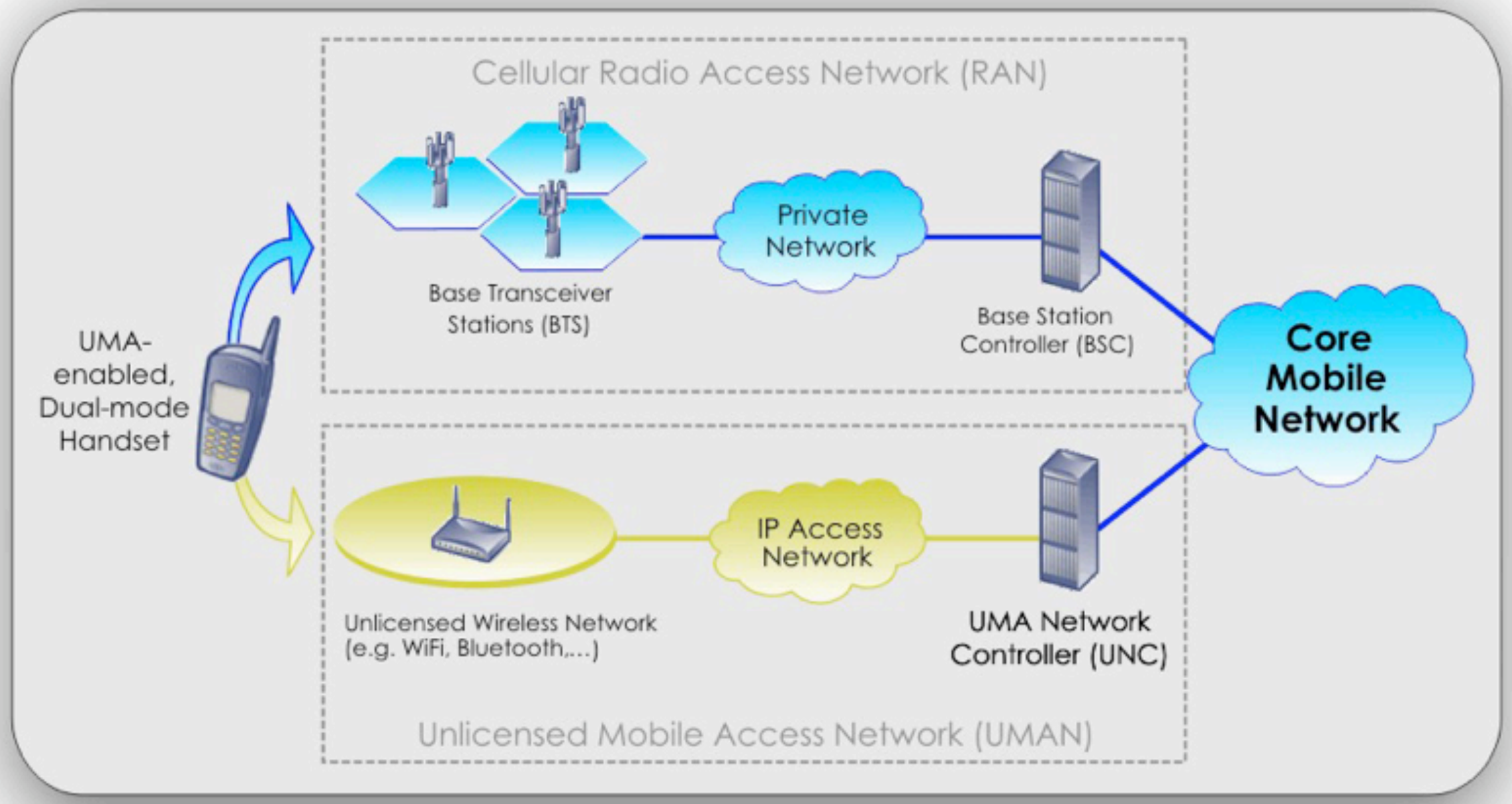
In reality...

- Much “hidden” shared infrastructure
  - DNS, web, NAT, TFTP, DHCP/PPPoE, Int/DiffServ, firewalls,...
- Emergent properties
  - example: web-based UI poisoning through SIP-field manipulation
- Real-time aspect makes problems harder
  - e.g., how can we filter voice spam based on content?

Unlicensed Mobile Access (UMA)

- Route GSM calls over the Internet (or a public network)
  - (usually) transparent handover between GSM and UMA
- Popular with cellphone providers
  - T-Mobile USA, Orange France, ...
- Benefits
  - reduce need to install expensive cell towers / upgrade capacity
  - reduce spectrum needs / utilization
  - improve “reception” in difficult locations
  - depending on billing, avoid roaming charges (think international!)
- Not to be confused with pico-/micro-/femto-cells

UMA deployment



Source: http://www.umatechnology.org/

UMA details

- Encapsulation of GSM/3G inside IP
  - complete frame, minus the on-the-air crypto
  - can transfer voice, IM and (in the future) video

- Typically, devices are WiFi-supporting cellphones
  - not strictly necessary, e.g., T-Mobile@Home in USA

- GSM frames are not natively protected
  - A5/2 is anyway weak (i.e., broken)

UMA security

- Handset-to-provider IPsec
  - strong crypto and integrity protection
  - key management (IKE, IKEv2) is a different story altogether
  - authentication done via EAP-SIM (based on shared secret)

- The key management protocol (IKE/IKEv2) is complex
  - perhaps “too big” to be trusted
  - more importantly, easy to misconfigure
    - not as big a problem in a tightly managed environment such as cellphones
    - but, UMA+smartphones smells trouble

- Provider needs to interface internal network with Internet
  - higher risk of compromise by external attackers
  - large numbers of potentially malicious insiders (i.e., legitimate users)

Threats in VoIP systems

- Everyone thinks of the traditional C/I/A threats
- Loss of communication confidentiality and privacy (C)
  - traffic analysis, content privacy

- Loss of communication integrity (I)
  - impersonation (inbound, outgoing calls), modification of content, falsification of call records

- Loss of communication availability (A)
  - accidental or intentional denial of service (DoS)

Unique VoIP characteristics

- Elaborate billing infrastructure in place
- Users are used to paying for telephony services
- Most charges are for relatively small amounts
- Large number of charges per billing cycle
  - unlikely that small unauthorized charge will be noticed or challenged
- Phone infrastructure is “trusted” by average user
  - perception carried over from PSTN
  - not grounded on facts or experience

VoIP-specific threats

- Theft of service
  - toll fraud
  - billing fraud
- Social engineering
  - phishing/spear-phishing made even easier
- Direct charge-back
  - immediate monetization

VoIP/IMS risk vectors

- Variety of risk vectors
  - some in common with other types of systems
    - software vulnerabilities
  - some are very specific to IMS
    - protocol vulnerabilities
  - some are common, but are amplified by some IMS feature
    - large-scale phishing through impersonation or call hijacking

Adversaries

- Who would launch attacks?
  - amateur blackhat
  - professional blackhat
  - fraudster
  - corporate competitor
  - national intelligence/espionage
    - recall 2006 wiretapping scandal in Greece
  - cyberwarfare
  - private investigator
  - ...

- Due to increased access (relative to PSTN), larger attack surface and larger number of potential attackers

Example of toll fraud attack

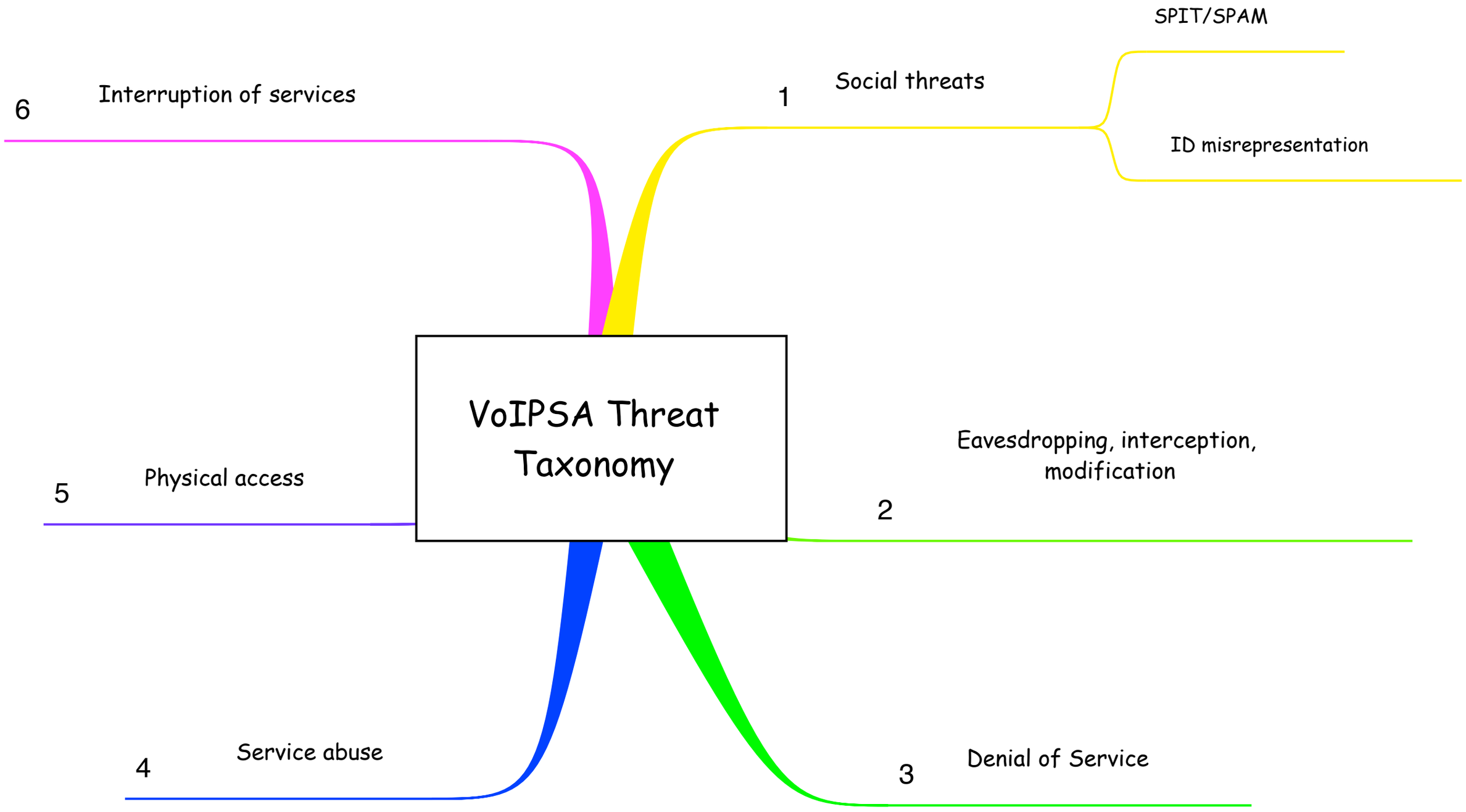
- Break into company PBX
  - use them to route calls of your customers
  - this has actually happened

http://www.theregister.co.uk/2006/06/08/voip_fraudsters_nabbed/
http://www.theregister.co.uk/2009/02/11/fugitive_voip_hacker_arrested/

"Federal authorities yesterday arrested a Miami man who they said made more than $1 million in a hacking scheme involving the resale of Internet telephone service."

"In all, more than 15 Internet phone companies, including the one in Newark, were left having to pay as much as $300,000 each in connection fees for routing the phone traffic to other carriers without receiving any revenue for the calls, prosecutors said."

VoIP Security Alliance taxonomy



VoIP vis. risks

- Confidentiality
  - in some protocols, attackers can easily eavesdrop
    - variety of available attack tools, e.g., VoMIT
    - particularly a problem with SIP/RTP
      - S-RTP defined, but largely unused
      - key management problem still unsolved (where's my PKI?)

- Integrity
  - software vulnerabilities
    - for example, as vulnerable to buffer overflows as any other piece of software
    - silver lining: even simple devices are generally designed for updateability
      - mixed blessing, update mechanism can be hijacked (usually based on TFTP!)

VoIP vis. risks

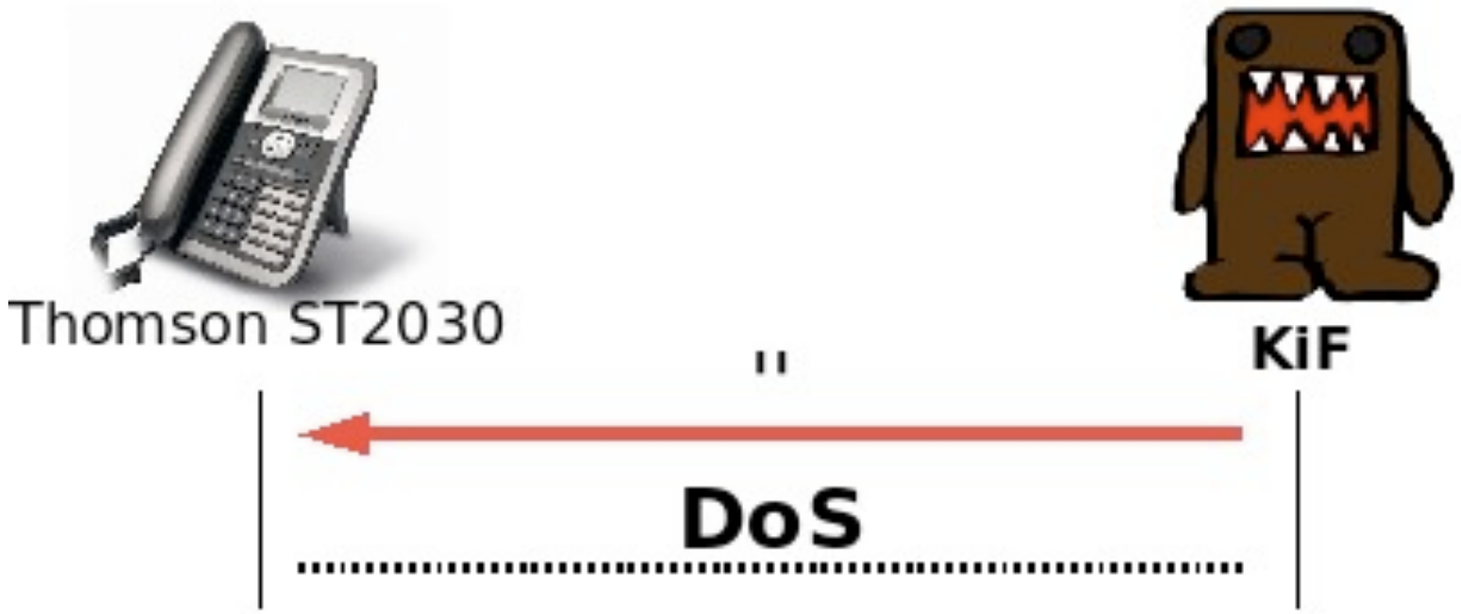
- Availability
  - susceptibility of equipment to denial of service
    - general network-borne DoS attacks, powerline, ...
  - how do you call someone to fix your problem?!

IMS-specific problems

- Architectural and protocol vulnerabilities
  - SIP device interactions (see following slides)
    - silent “snooping” via multipresence
    - fraud
      - bill bypassing
      - hijacking of someone else’s account/PBX
  - protocol-specific denial of service attacks
    - malformed messages
    - call routing games
  - separation between signaling/data transport can be leveraged
    - induce someone’s phone device to act as a DoS zombie
    - incriminate an IP address/person

Trivial protocol-specific DoS attack

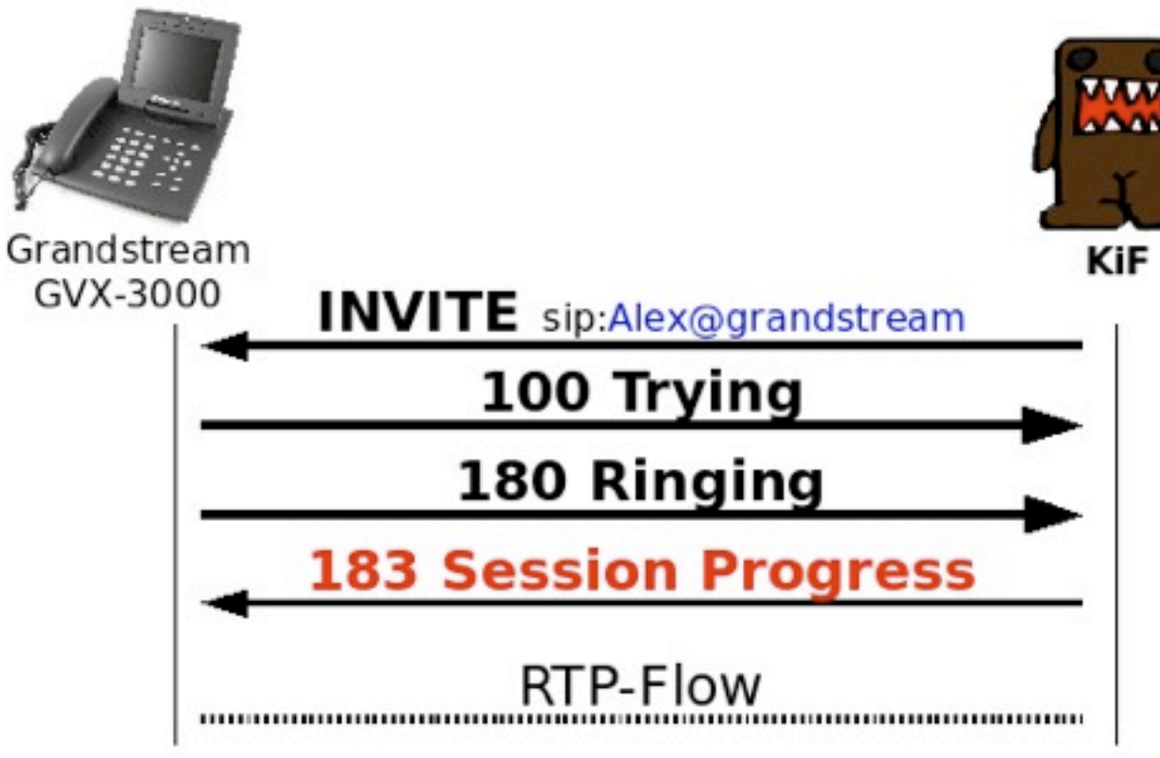
- Single packet “phone kill”



Vulnerability by KiF
CVE-2007-4753

Privacy attack

- Call someone, then report “call in progress” before ring
  - turns phone into eavesdropping device!



Vulnerability by KiF
CVE-2007-4498

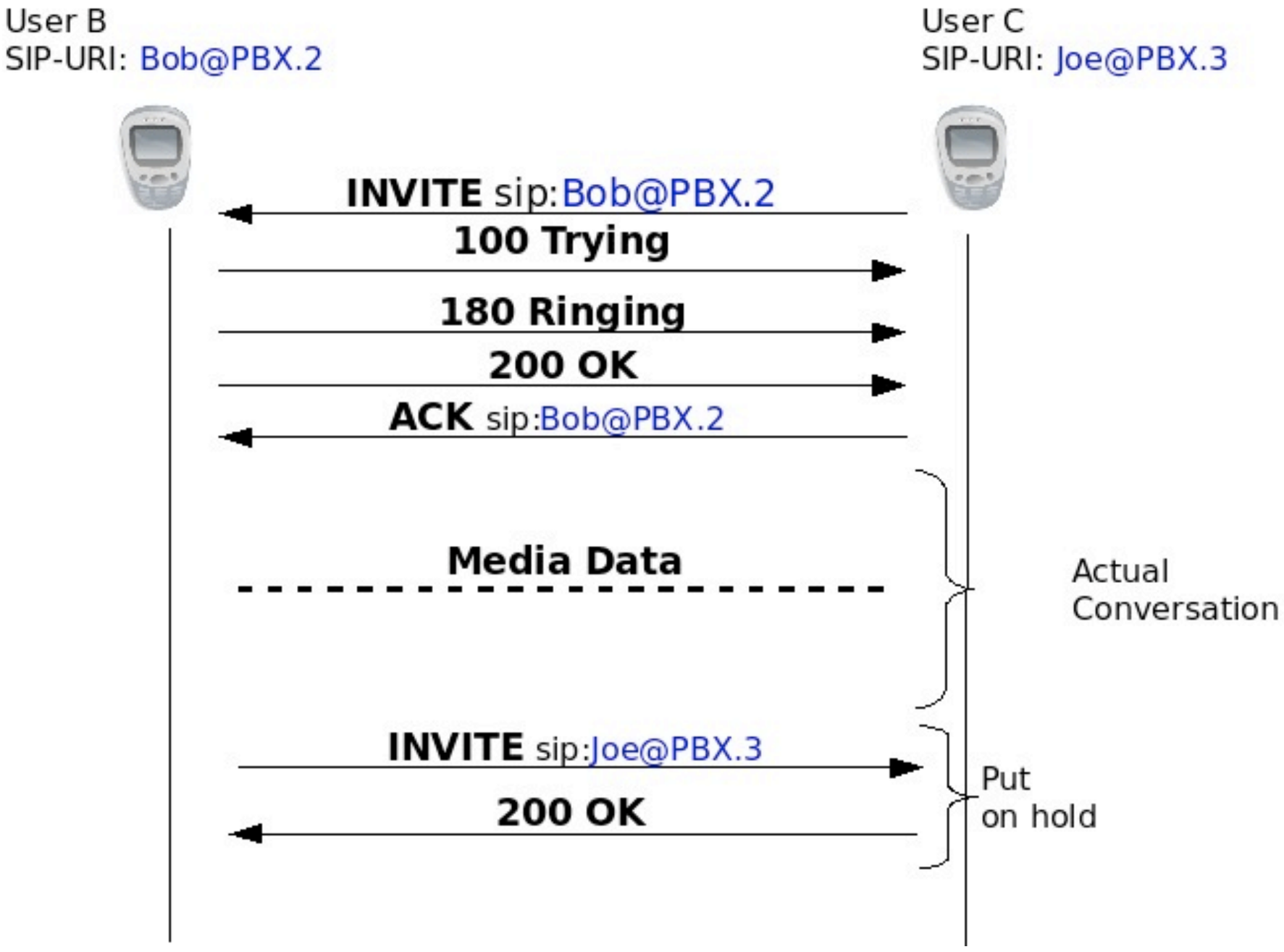
Billing avoidance and XSS attacks

- SQL injection that targets the PBX's billing records

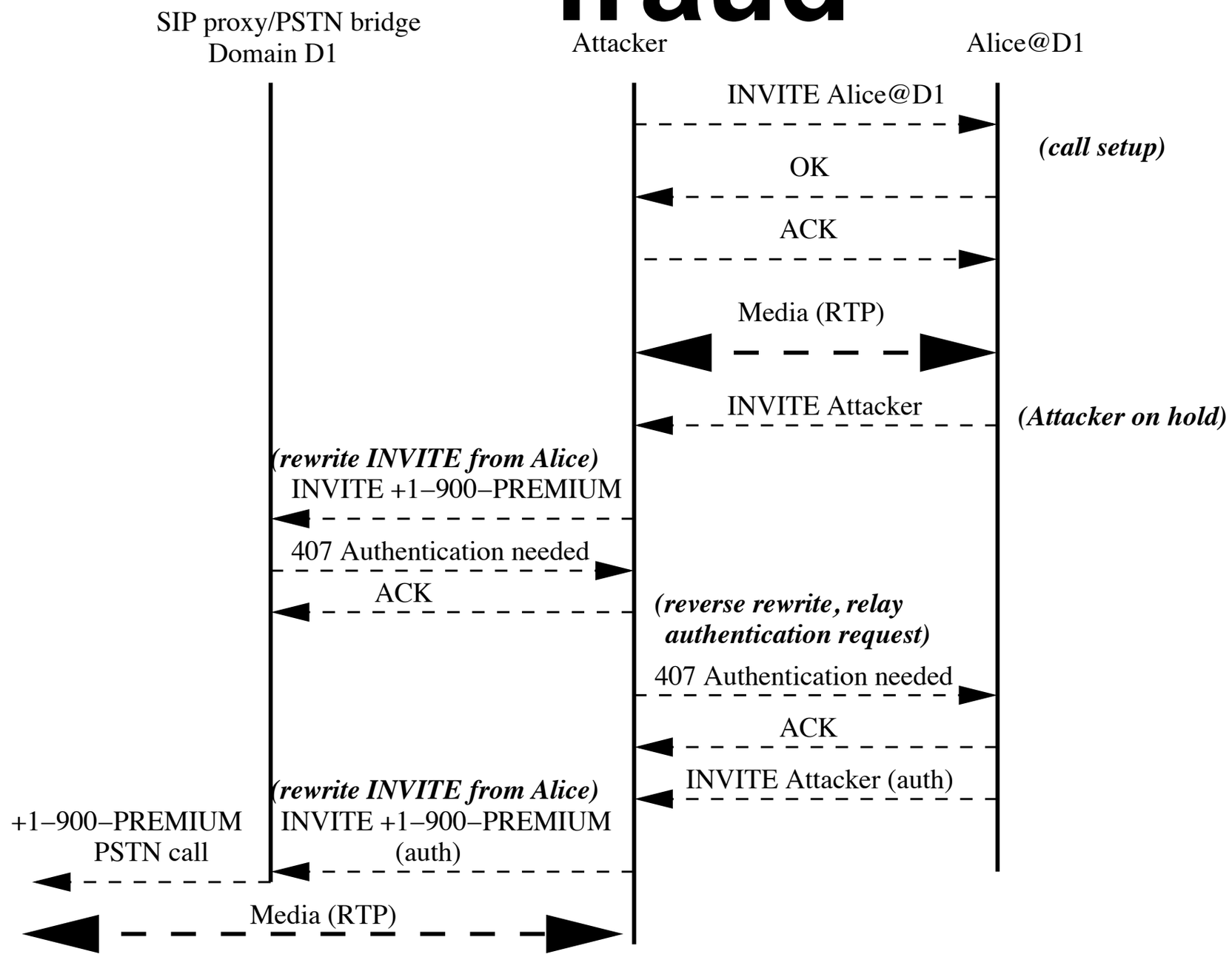
- SQL-enabled XSS attack that targets administrator or user viewing call logs with browser!

Vulnerability by KiF
CVE-2007-54881

Reminder: call forwarding



Protocol games: toll fraud



draft-state-sip-relay-attack

Hybrid threats

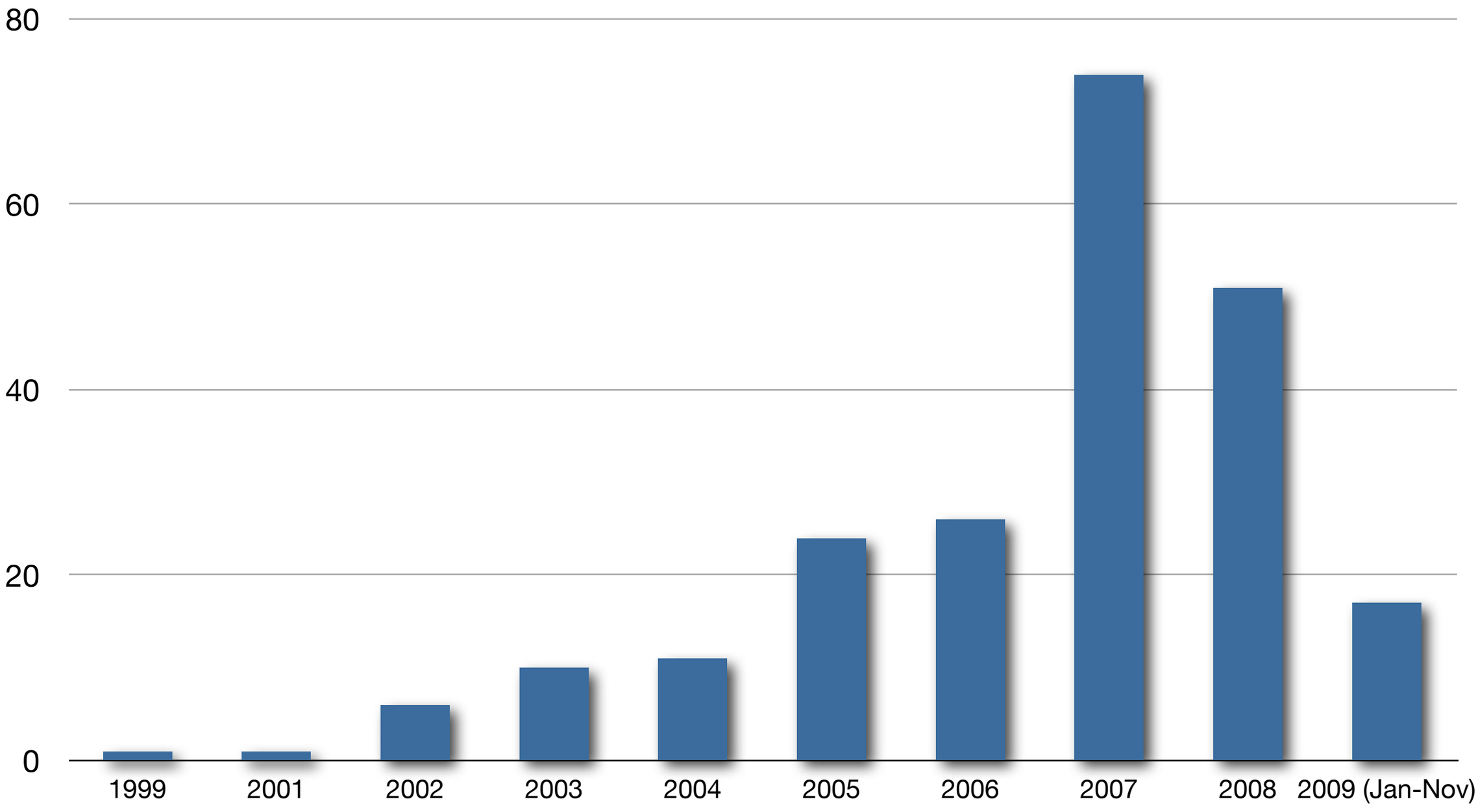
- Generic threats made easy/enabled by IMS architecture
  - more realistic phishing/spear-phishing
    - common attack: call by “bank officer” asking for personal information
      - remember: CallerID easy (trivial) to spoof
    - (somewhat) more complicated attack: compromise SIP signaling to catch the “callback” from customer to the bank!
      - compromise of company SIP-PBX or end-device
      - router- and routing-based attacks
      - DNS poisoning

- Configuration problems
  - many options, many devices: easy to misconfigure

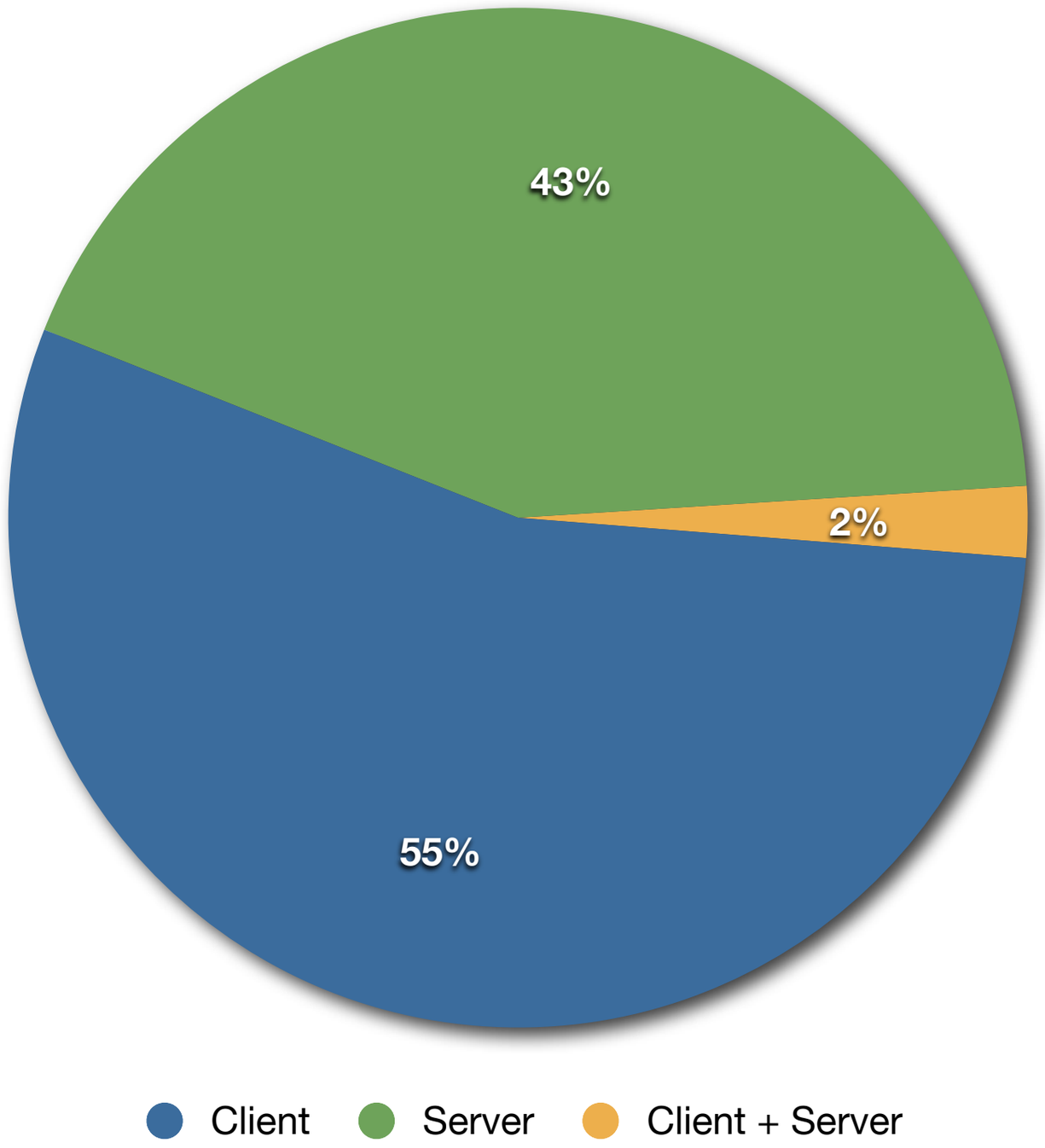
Vulnerability Survey

- Looked at 221 publicly disclosed vulnerabilities on VoIP & SIP
  - listed at the Common Vulnerabilities and Exposured (CVE) database
    - http://cve.mitre.org/
- Classified them according to three criteria
  - VoIPSA taxonomy
  - Confidentiality/Integrity/Availability (CIA) violation
  - Implementation/Configuration/Protocol vulnerability

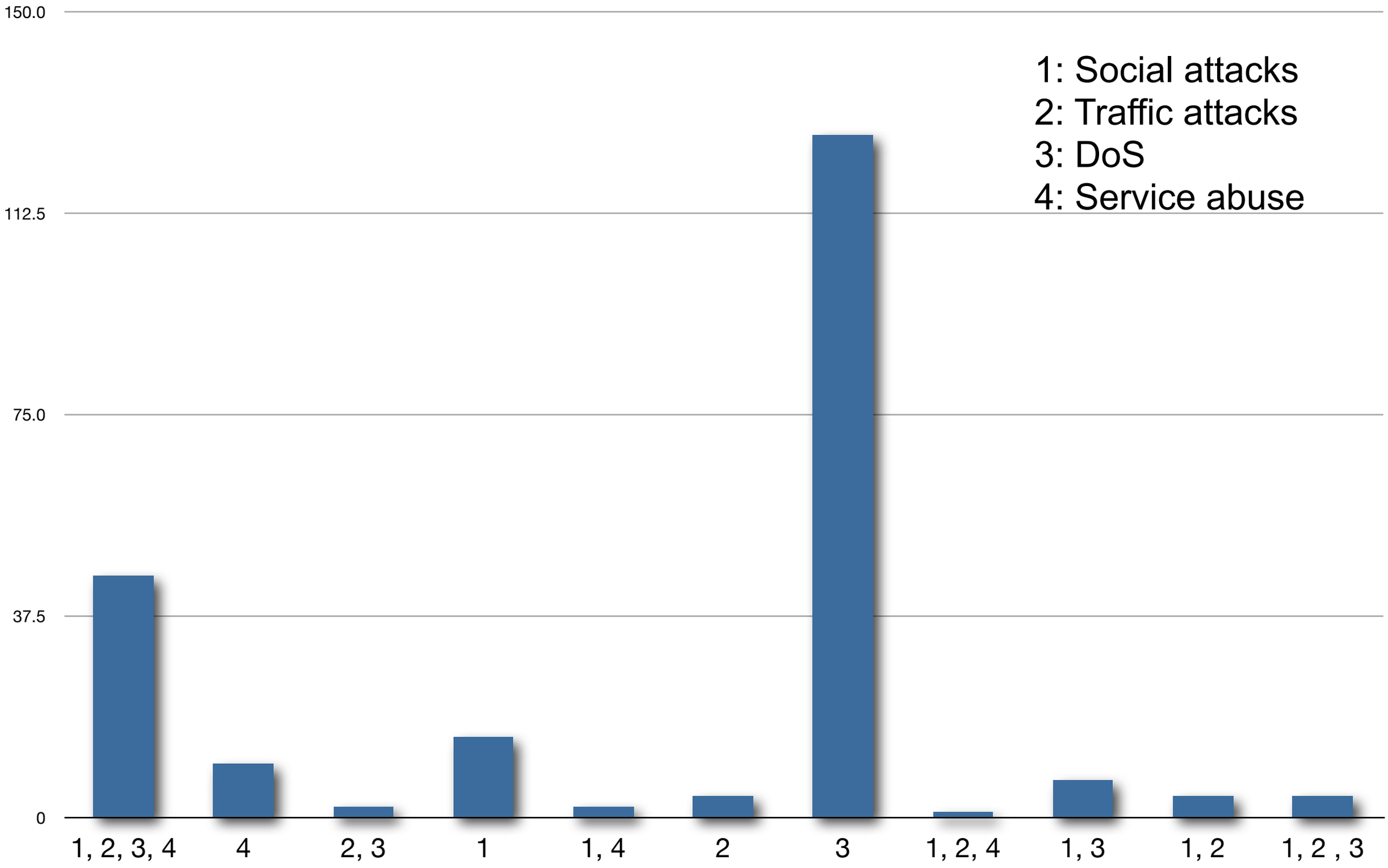
Vulnerabilities/year



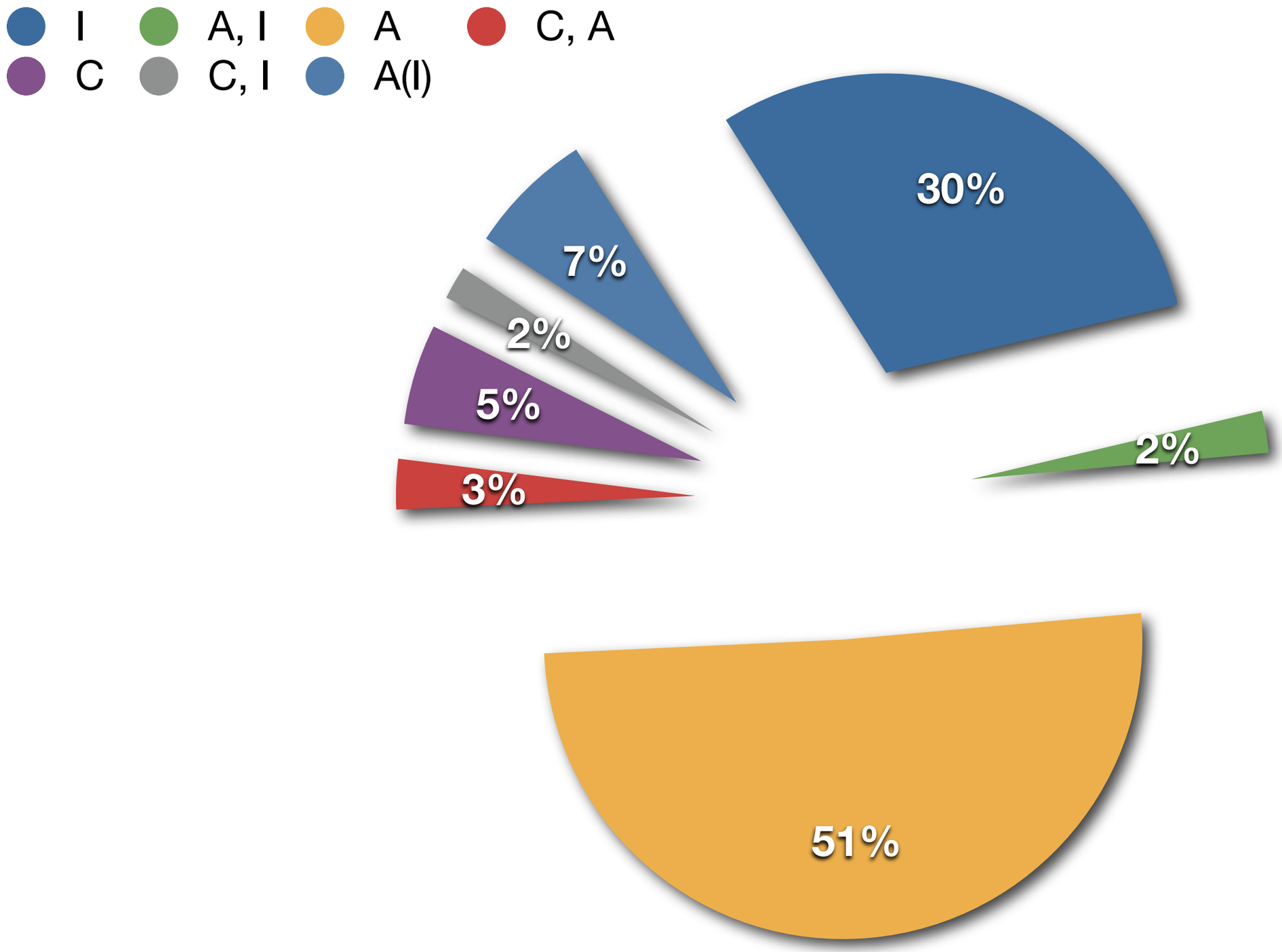
Client vs. Server



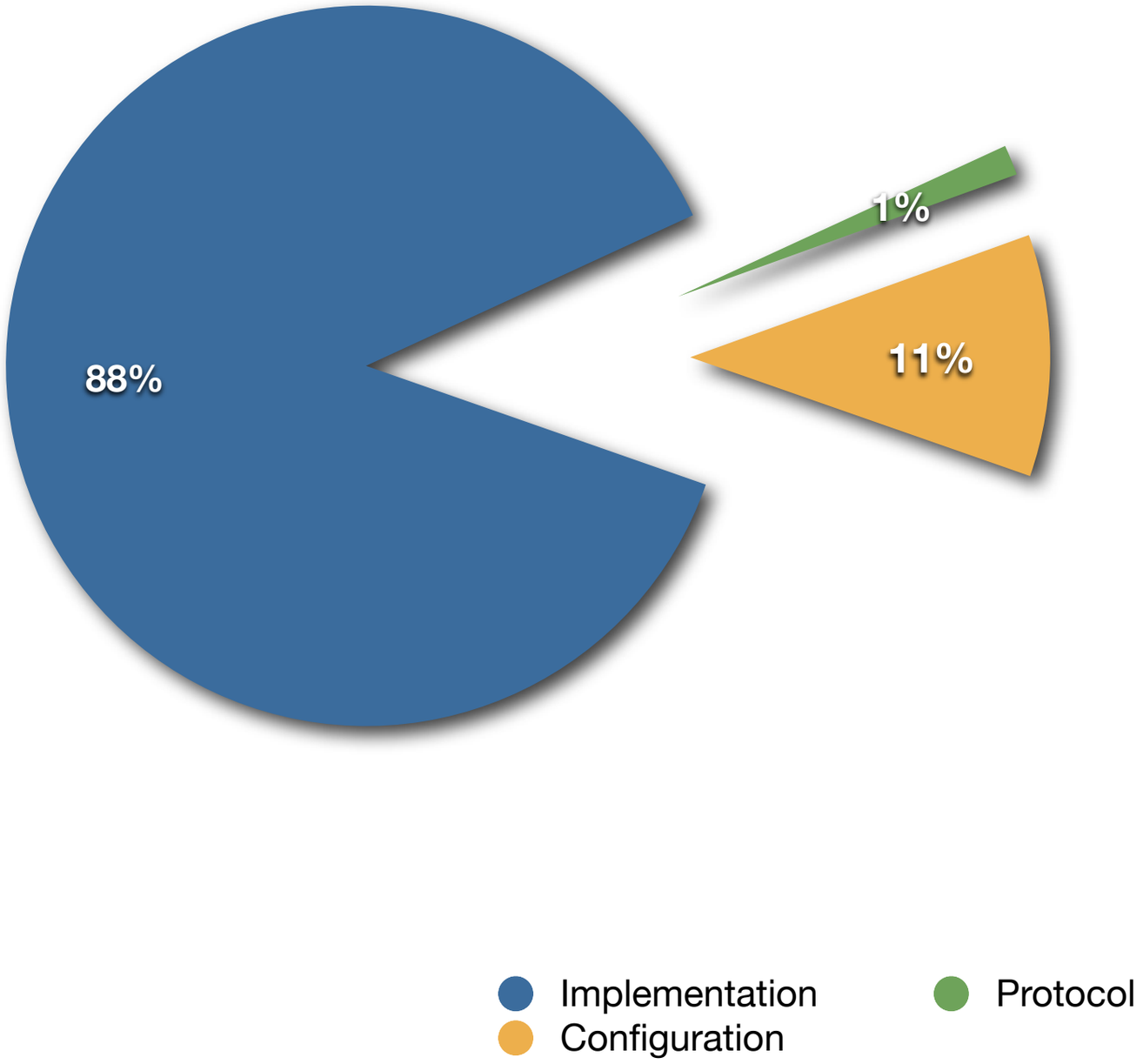
VoIPSA classification



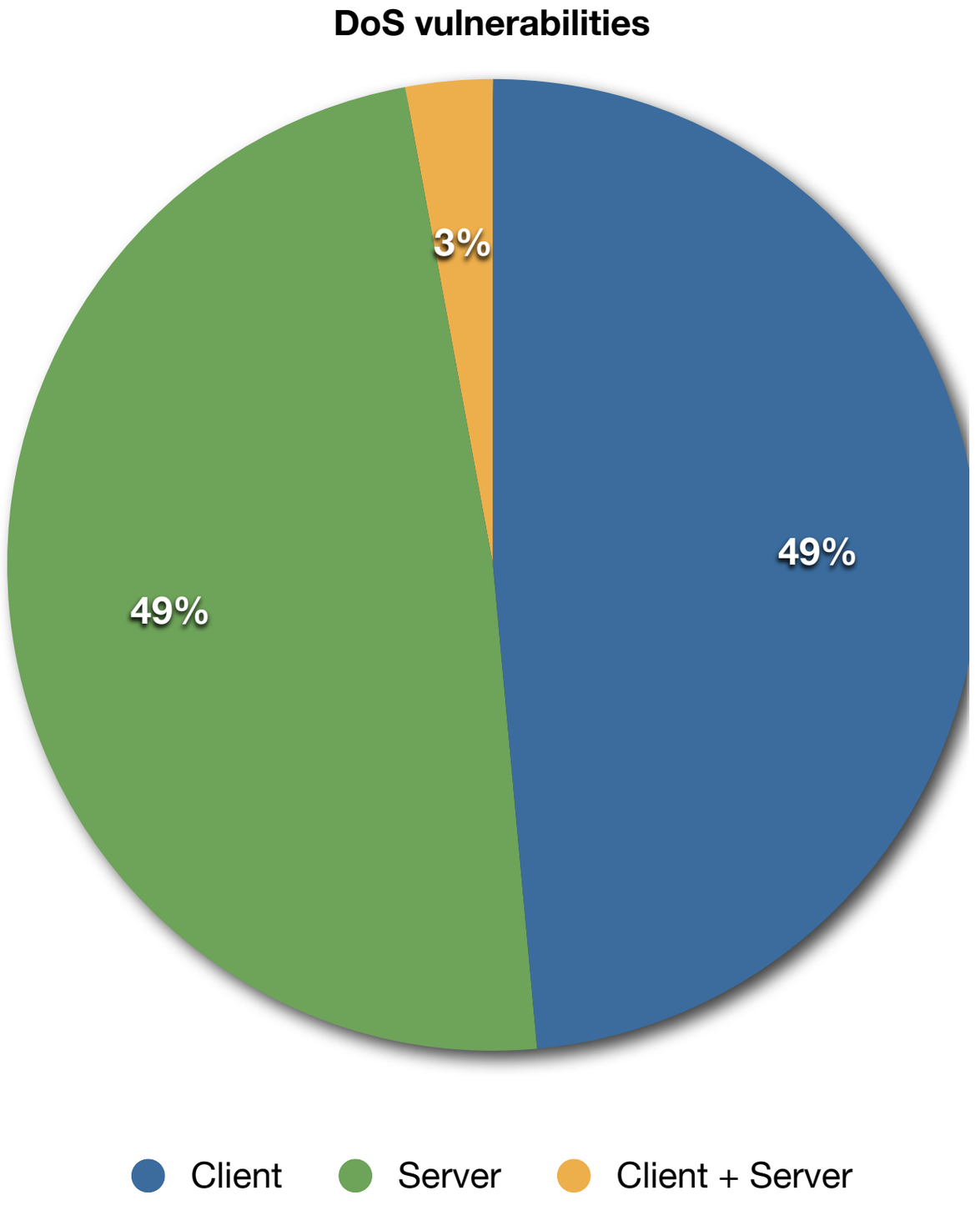
CIA classification



ICP classification



DoS breakdown



Other insights

- Only 3 out of 221 vulnerabilities could be mitigated by the user
  - all others required action by the manufacturer
- 55+ out of 221 vulnerabilities involved cross-protocol interaction bugs
  - most commonly (19/55) through HTTP/web server on device
- 10+ bugs involved default passwords or bad/no authentication
- 3 systems had remotely accessible debuggers running
- 8 vulnerabilities on VoIP-handling component of firewalls or security appliances

Thoughts

- We worry about loss of confidentiality
  - data shows that primary threat is about availability
- Implementations are particularly weak
  - rife with buffer overflows, XSS, CSRF, and other code-injection vulnerabilities
  - lessons for protocol designers?
- Weak default configurations
  - debuggers, unauthenticated privileged access, etc.
  - probably tip of the iceberg on site-specific configuration-based vulnerabilities

Thoughts (2)

- Protocol-level ambiguities and vulnerabilities exist despite many eyes scrutinizing the specifications

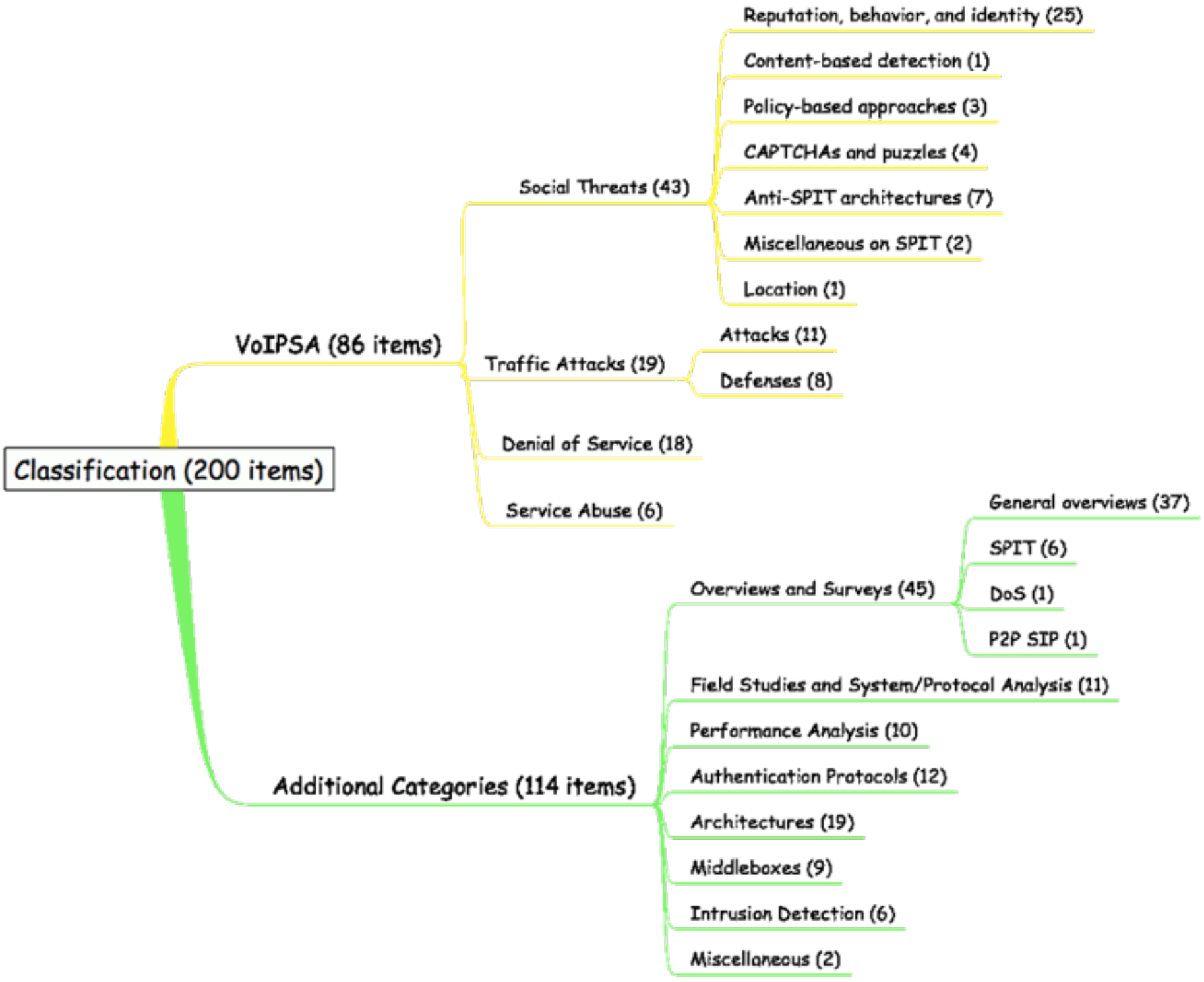
- Large number of cross-protocol vulnerabilities
  - how do we address such problems?

Research Paper Survey

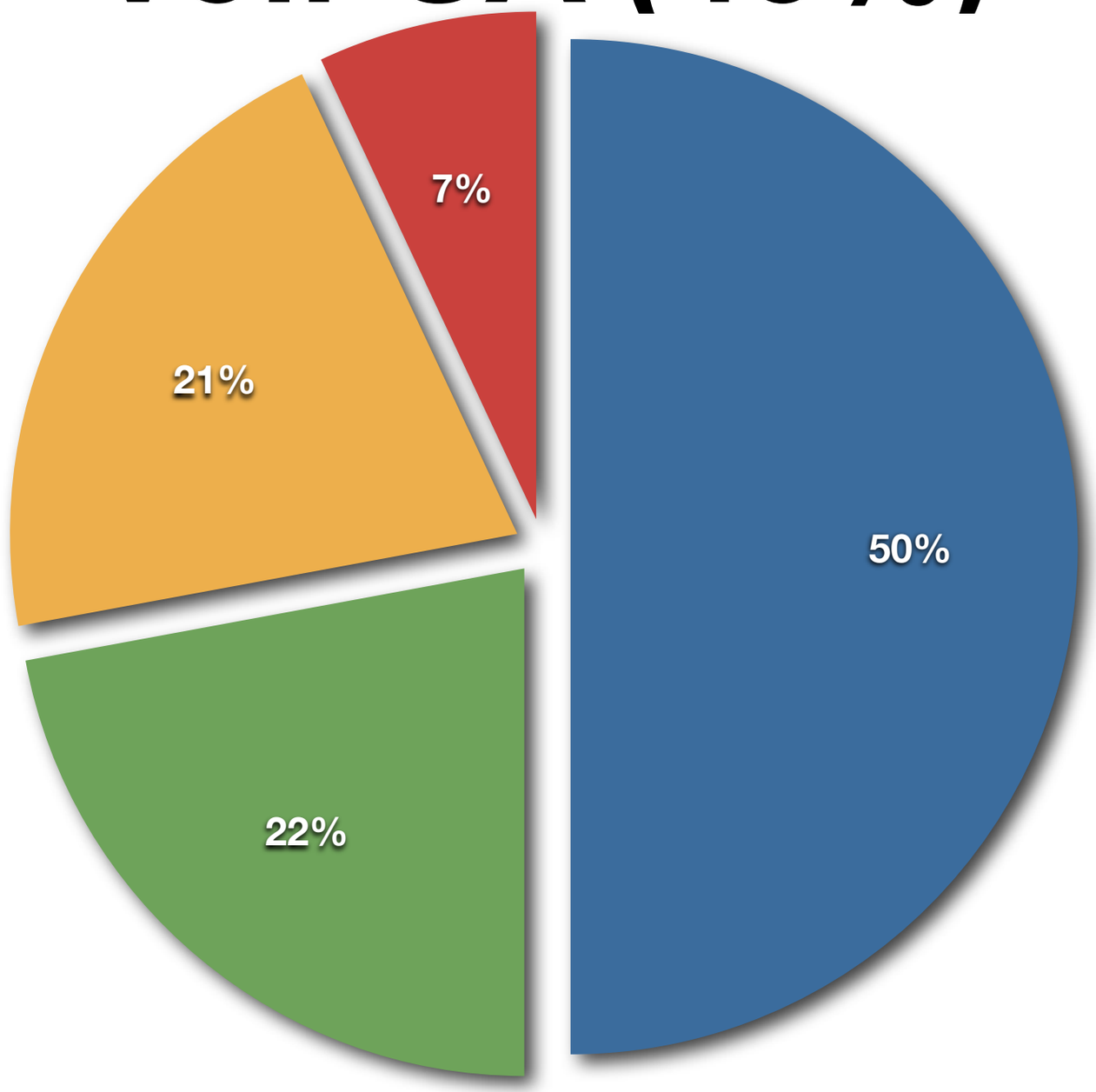
- What do we, as researchers, focus on?
  - Does it relate to the vulnerabilities that are reported?

- Conducted survey of 200 research papers
  - Conference, journals, workshops, plus a few white papers
  - Started from some known seeds, then recursively followed citations to relevant work, looked at prior/following years in same venue, used search engines
  - Group of papers forms a closure under cross-referencing
  - Paper in the ICISS proceedings is short version; longer version to appear in 2010

Paper classification

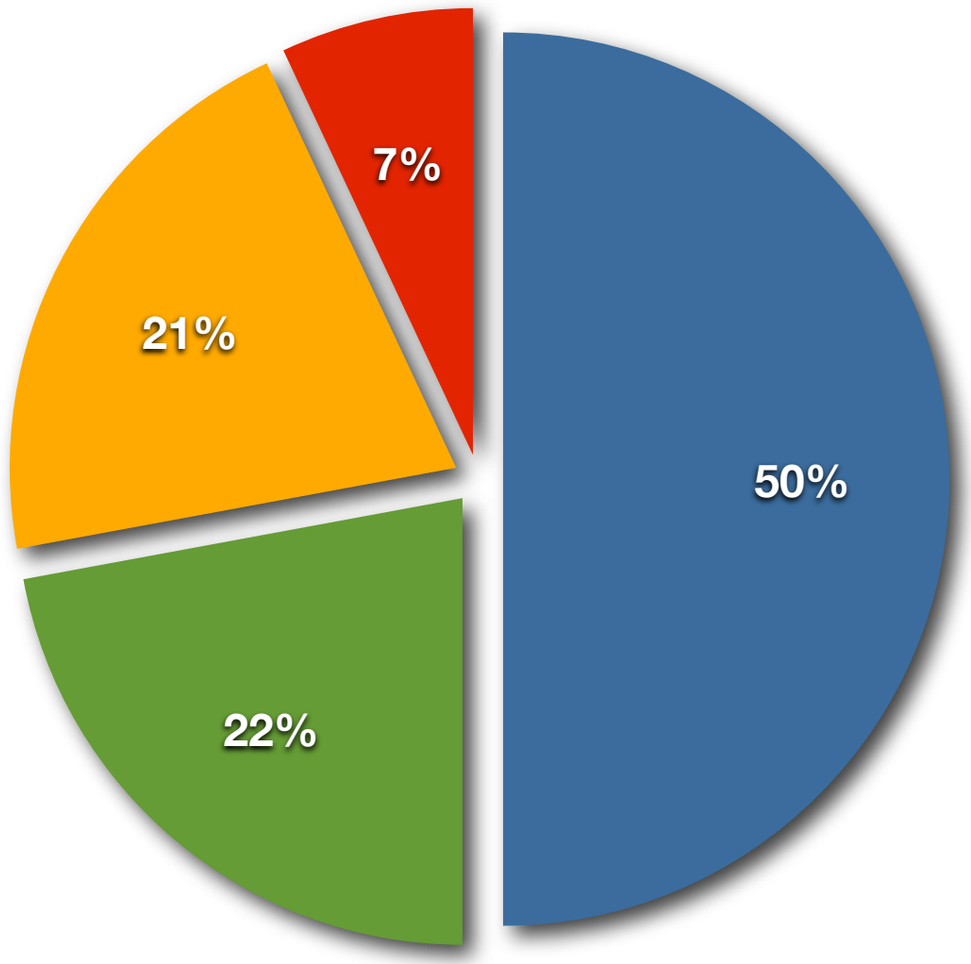


Paper classification per VoIPSA (43%)

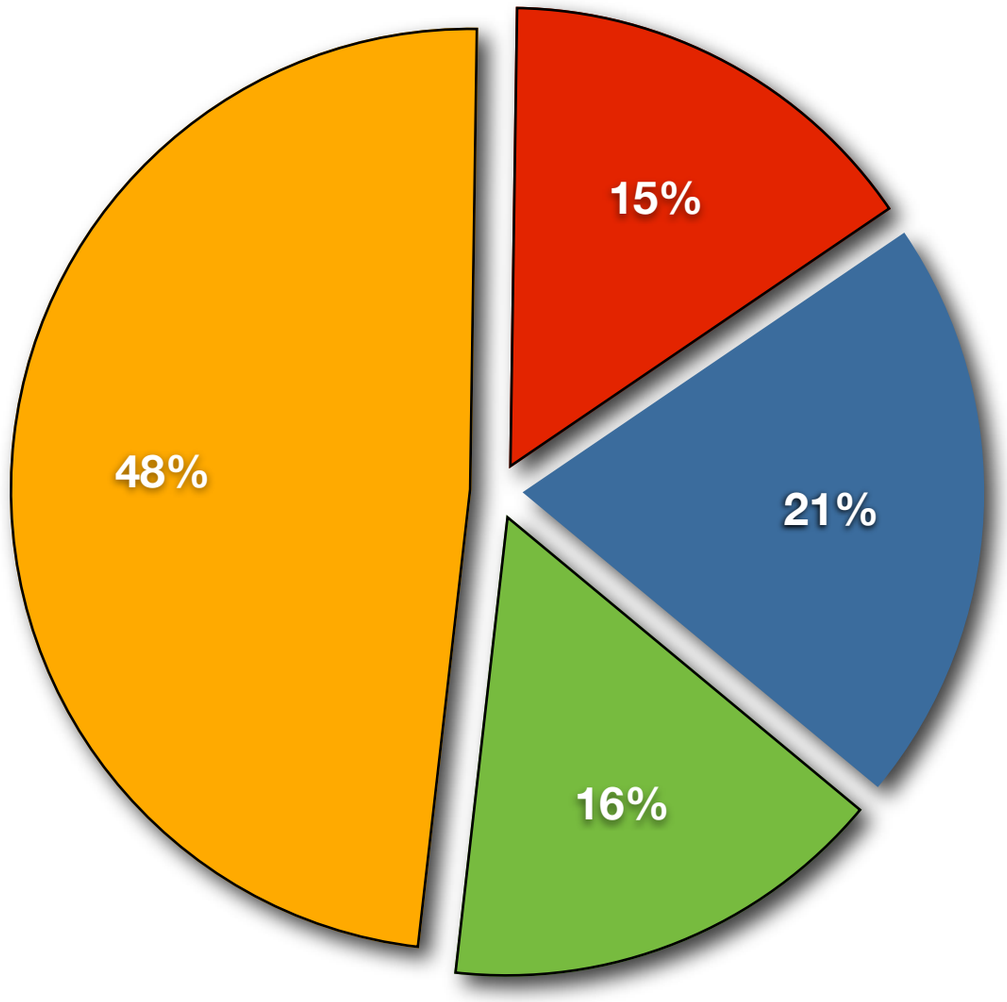


Comparison with Vulnerabilities

Research Papers

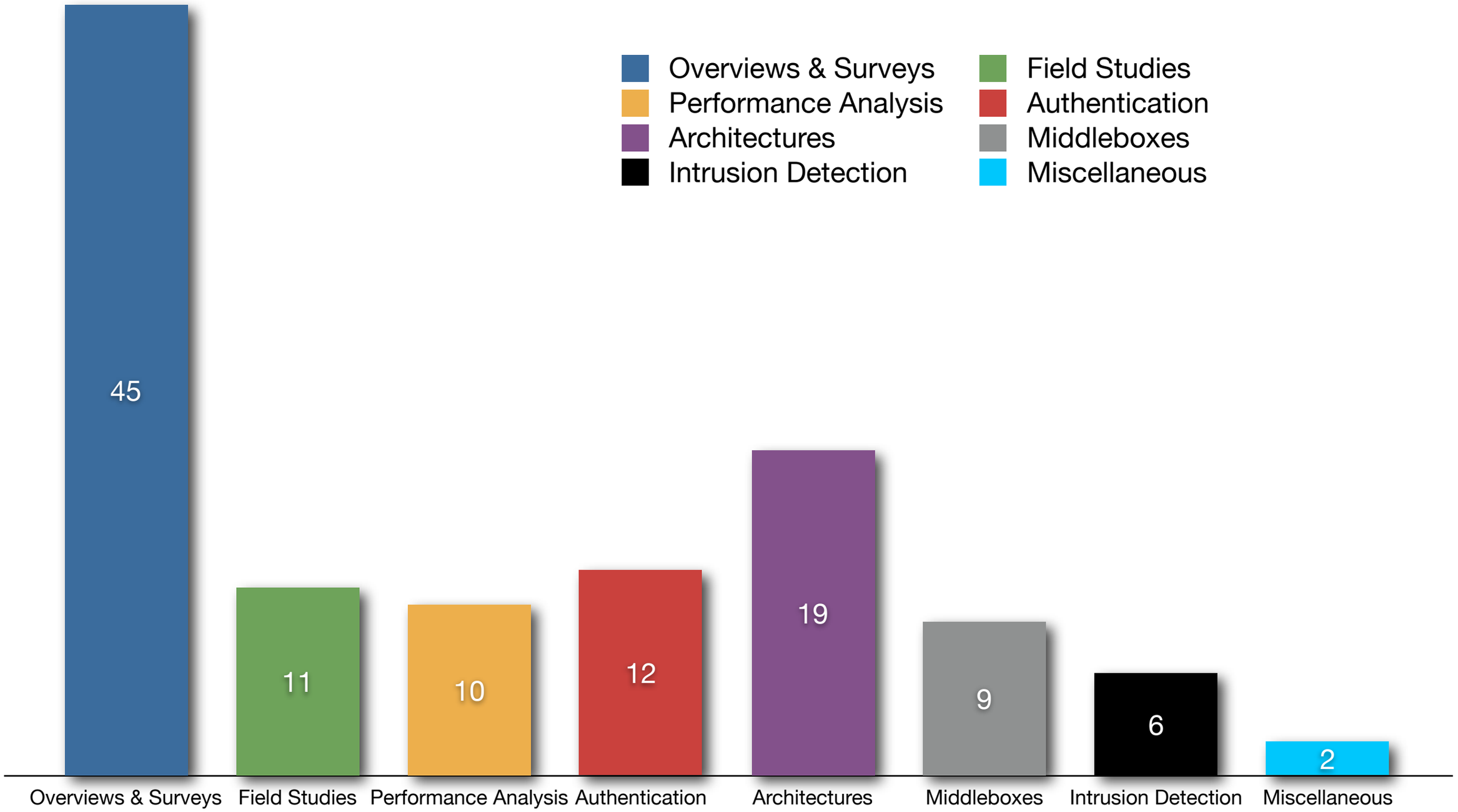


CVE Vulnerabilities



Social Threats (1)
Traffic Attacks (2)
Denial of Service (3)
Service Abuse (4)

Non-VoIPSA papers (57%)



Lessons

- A lot of work goes into SPIT prevention
  - We have not seen much of that in practice
    - the lesson of email SPAM well-learned?
  - But, SPIT isn't all there is to social threats!
    - not much else is being done, in terms of research

- Some work on service abuse is being done
  - Unsurprising, since abuse translates to $$$ lost
  - Statistics-only view can be misleading, however...

- Research severely under-investigates DoS vulnerabilities
  - Note that these are not the same as network DoS (flooding) attacks
  - Particularly worrisome given the vulnerability of both clients and servers
    - how do we do fault tolerance for a VoIP handset?

Big Caveat

- Both surveys represent “static” and abstract views

- We don’t really know what is happening in practice
  - What are the bad guys doing wrt VoIP devices/services, and how?
  - How successful are they?
  - Do they target VoIP service providers, enterprises, consumers, ... ?

- To know the significance of both the reported vulnerabilities and the research being done, we need to know the answers to these questions!

VAMPIRE project

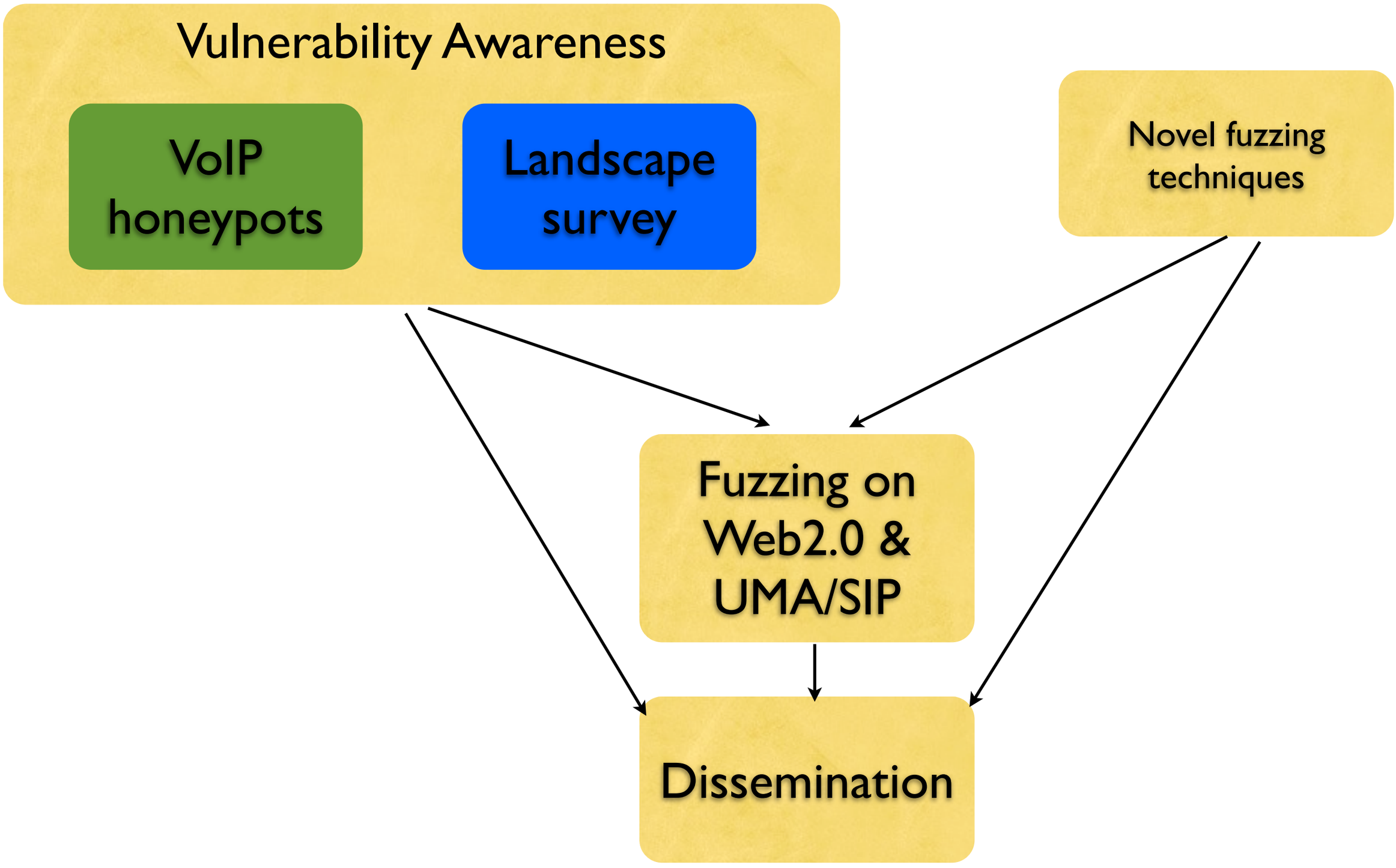
- Research project funded by Agence Nationale de Recherche (ANR; equivalent of US NSF)
  - duration: 3 years
  - start date: January 2009 (approximately...)

- Partners
  - INRIA (lead)
  - EURECOM
  - Symantec Research Labs Europe
  - Orange Labs (France Telecom)

Project goals

- *Design and experimentation of advanced vulnerability discovery methods based on smart fault injection -fuzzing- and passive host-level attack detection.*
  - Vulnerability awareness
  - Automated fuzzing of unknown protocols
  - Close-Loop fuzzing
  - Fuzzing frameworks assessment models
  - Application domains
    - SIP & Web 2.0 SIP interactions
    - IP Multimedia Subsystem

WP interactions



Vulnerability Assessment

- Guide our thinking in approaching the IMS security problem

- Static view: analysis of known vulnerabilities
  - you have seen some early work
  - also to come: analysis of research literature

- Dynamic view: behavior tracking of bad guys

VoIP honeypots

- Dynamic aspect of vulnerability assessment
- Develop techniques for lightweight emulation of IMS
- Track behavior of bad guys with respect to IMS

Dynamic view methodology

- Leverage ScriptGen
  - mechanism for “learning” protocol interactions
  - aimed at creating high-fidelity low-interaction honeypots
- Leverage and augment existing distributed honeypot infrastructure

SGNET

- Distributed honeypot deployment for the analysis of code injection attacks
  - How does malware propagate?
  - What kind of exploits are observed in the different locations of the Internet?

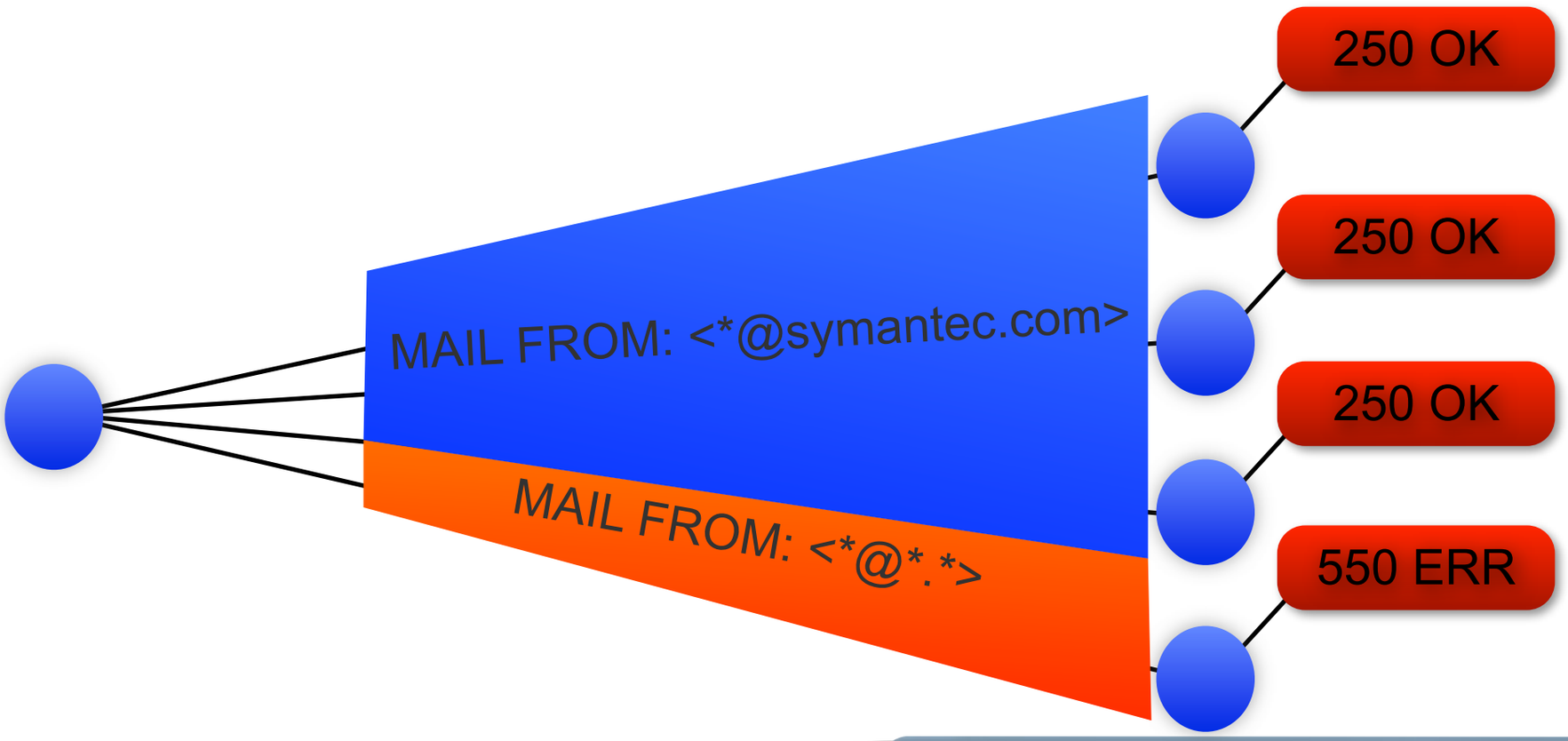
- Honeypot sensors distributed over the whole Internet
  - Deployed by volunteering partners
  - WIN-WIN partnership: hosting a sensor, the partner receives access to the whole data
  - Non-Disclosure Agreement to protect the identity of the participants, attackers and victims

ScriptGen

- Protocol-agnostic algorithm
- Observe conversation samples between a client and a real server
- Infer semantics using bioinformatics algorithms
- Proved good results in handling deterministic exploit scripts

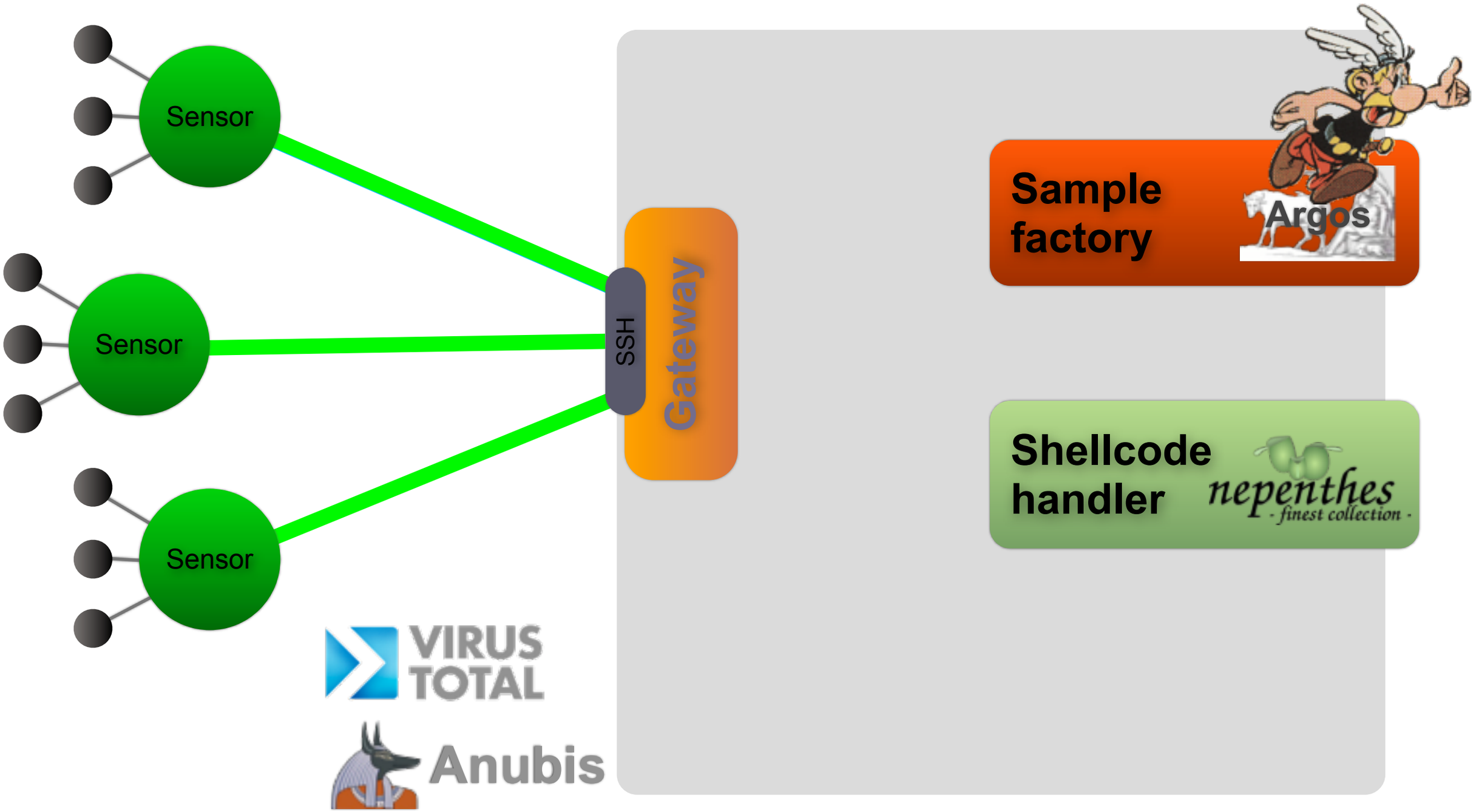
ScriptGen

- Protocol-agnostic algorithm
- Observe conversation samples between a client and a real server
- Infer semantics using bioinformatics algorithms
- Proved good results in handling deterministic exploit scripts



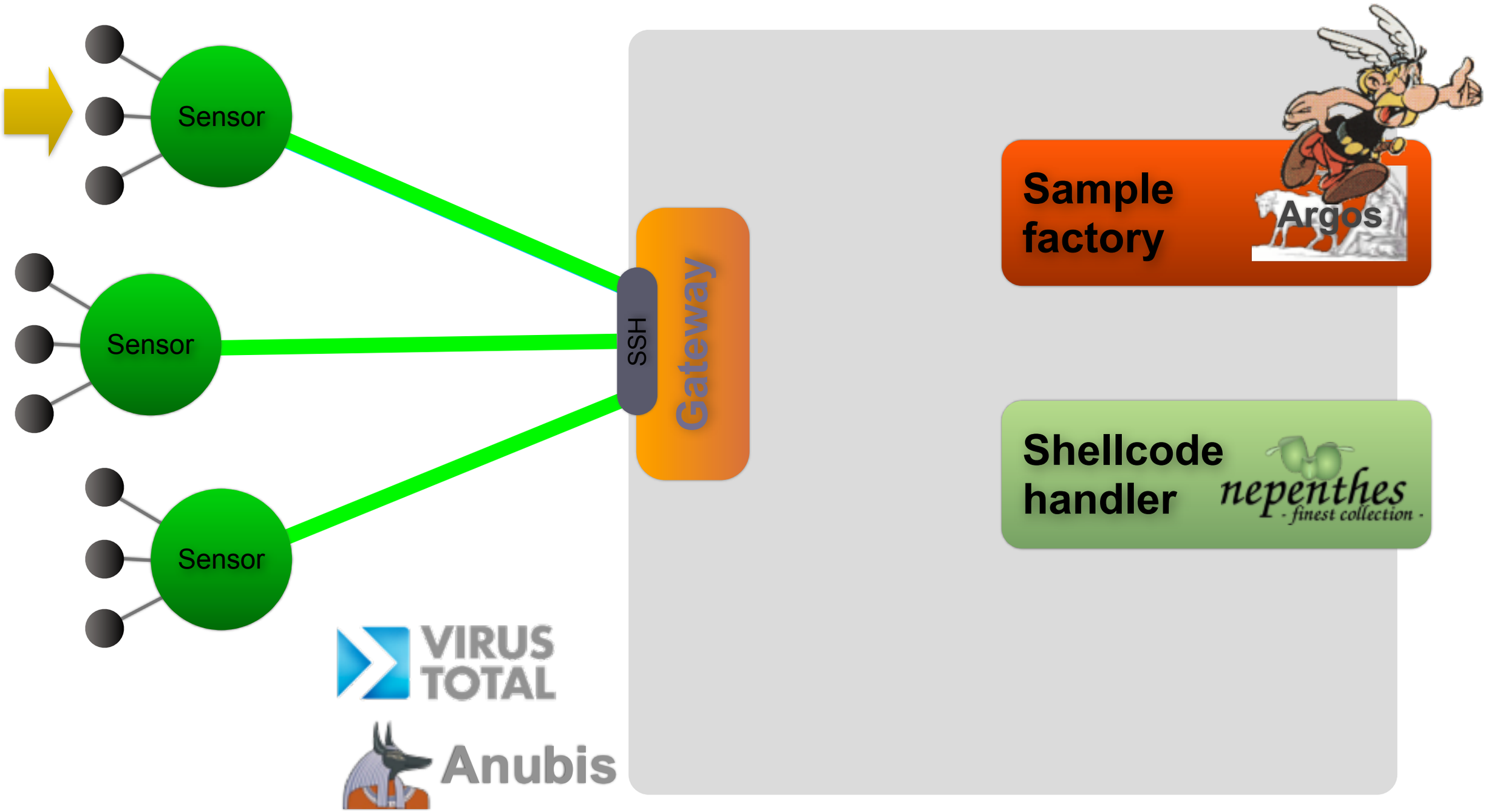
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



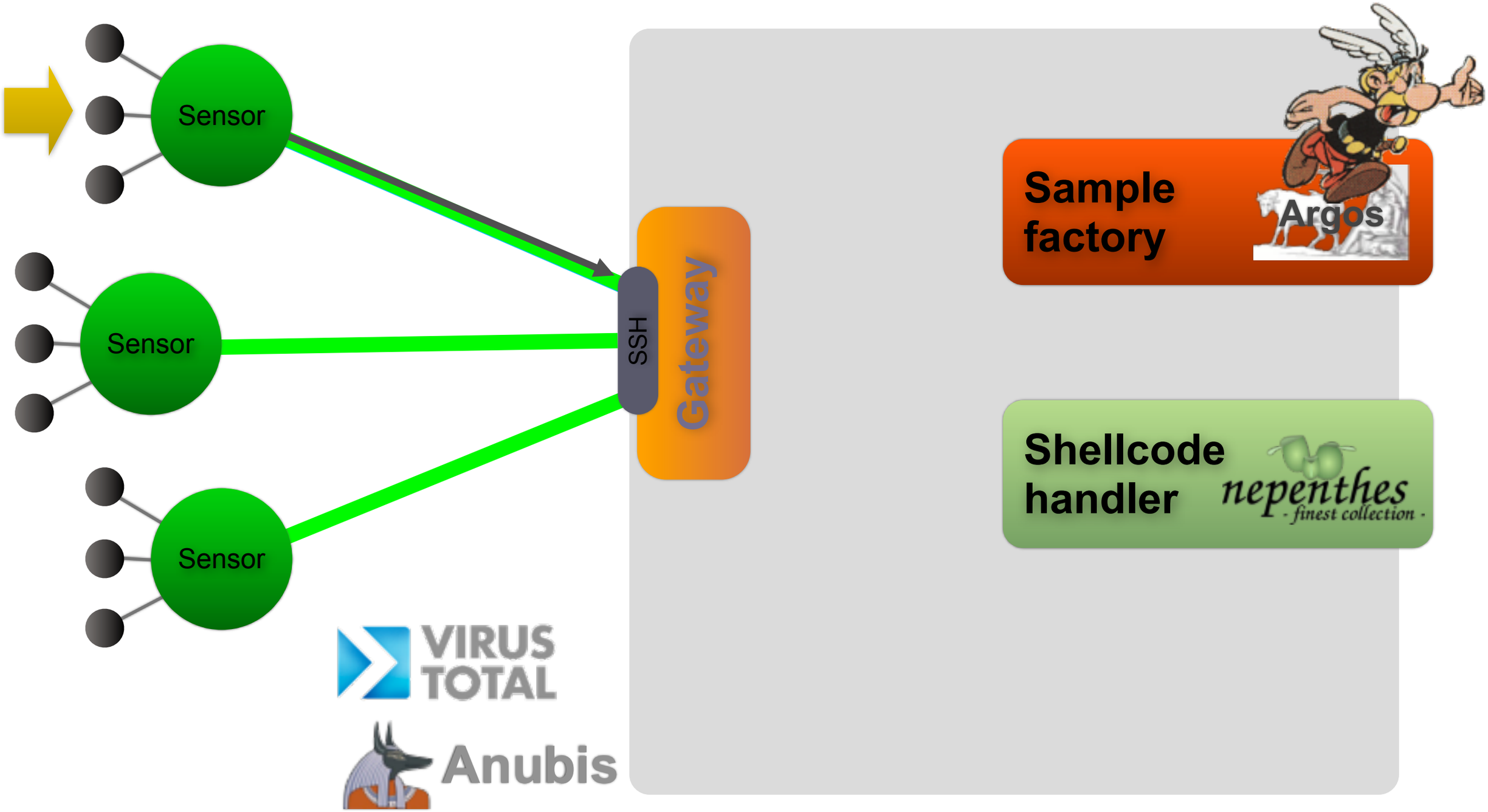
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



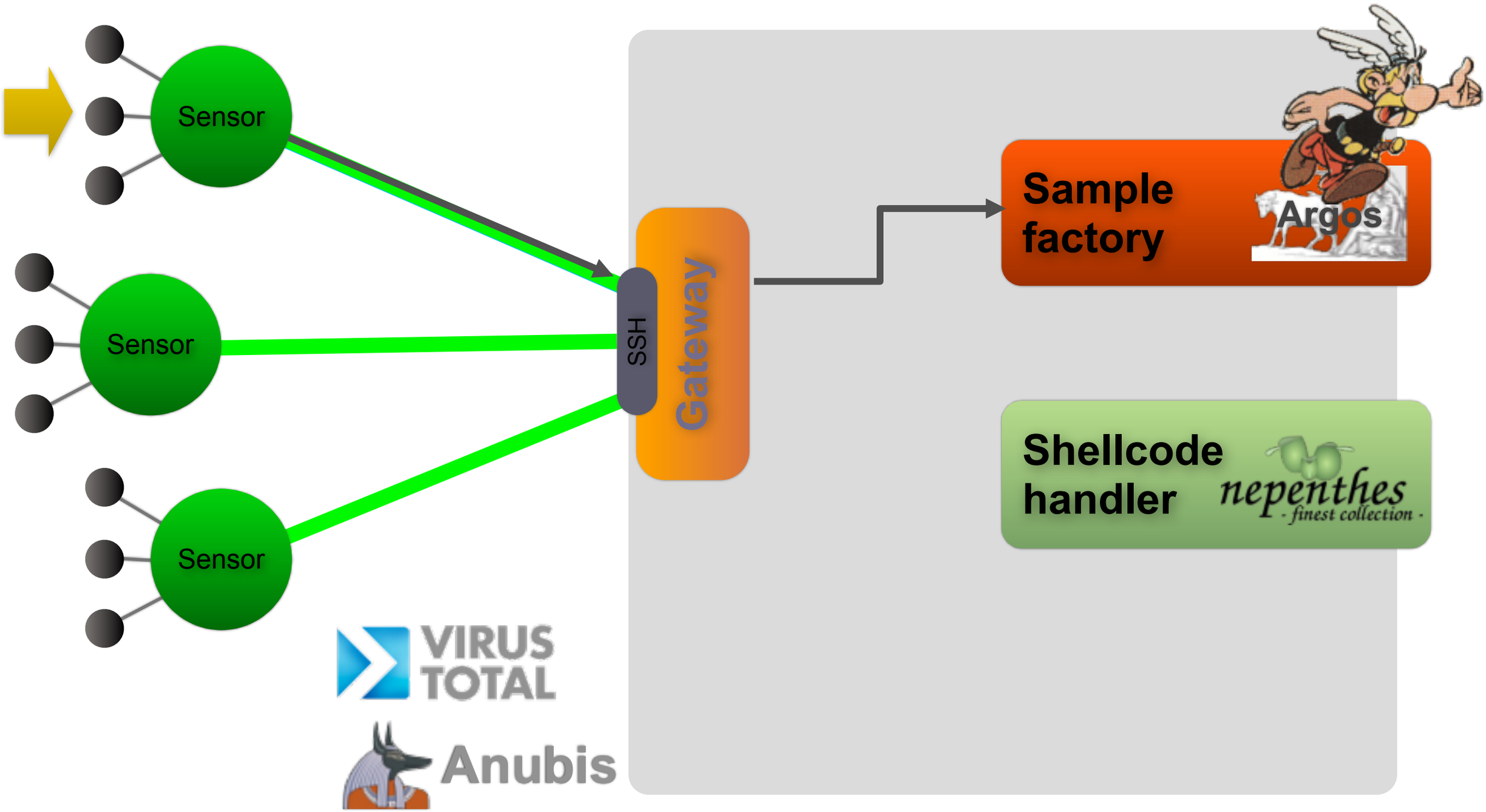
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



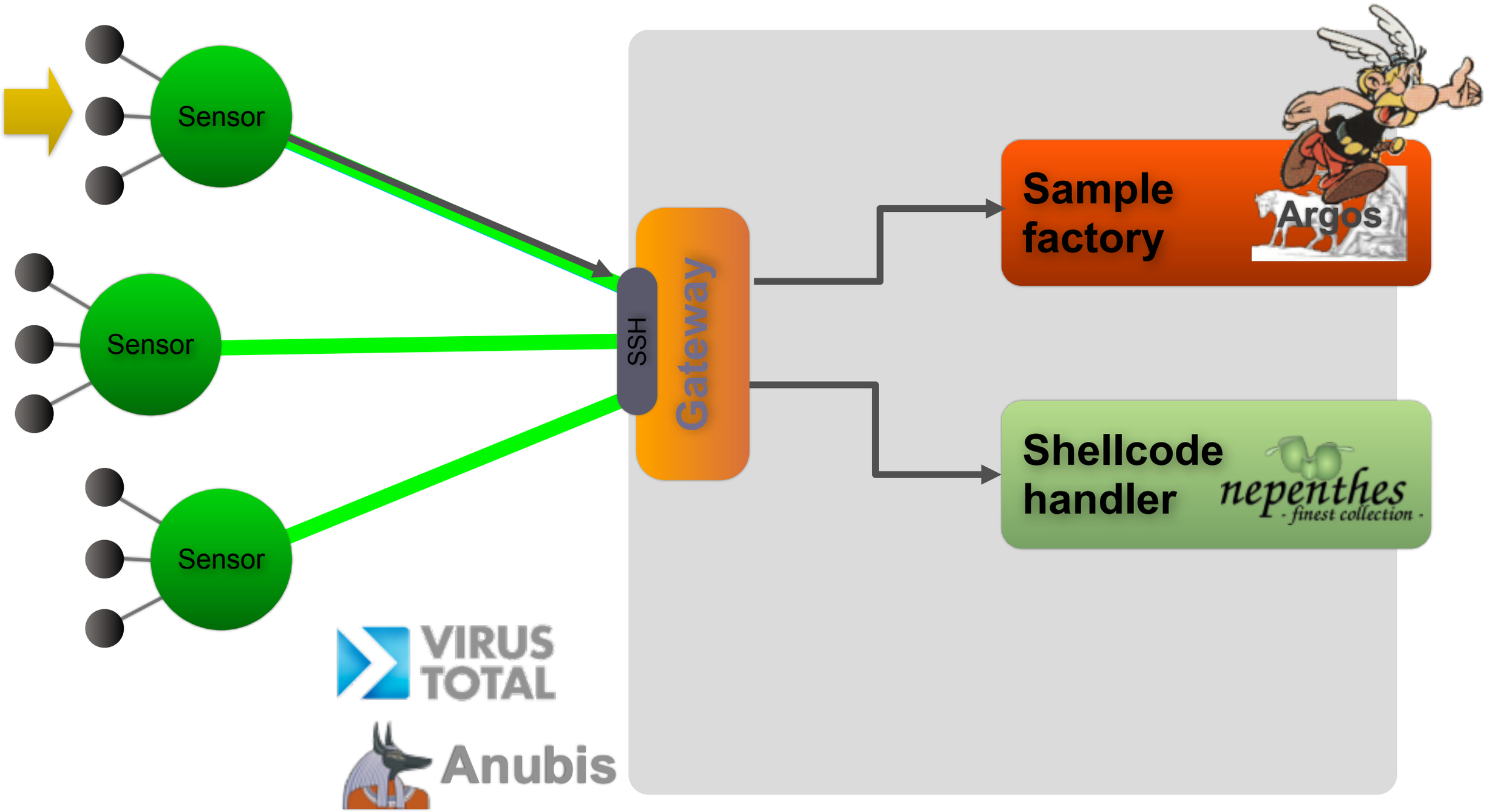
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



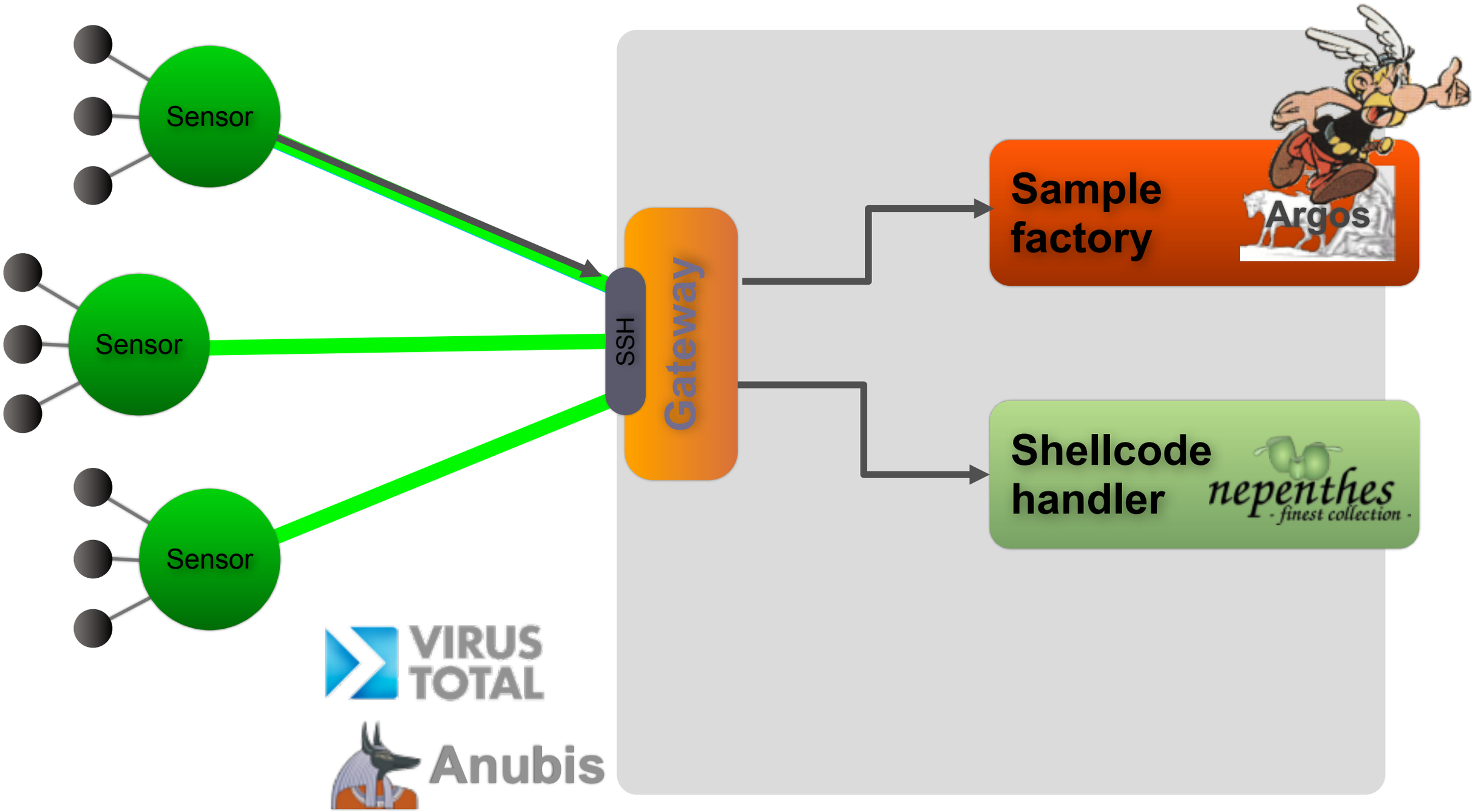
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



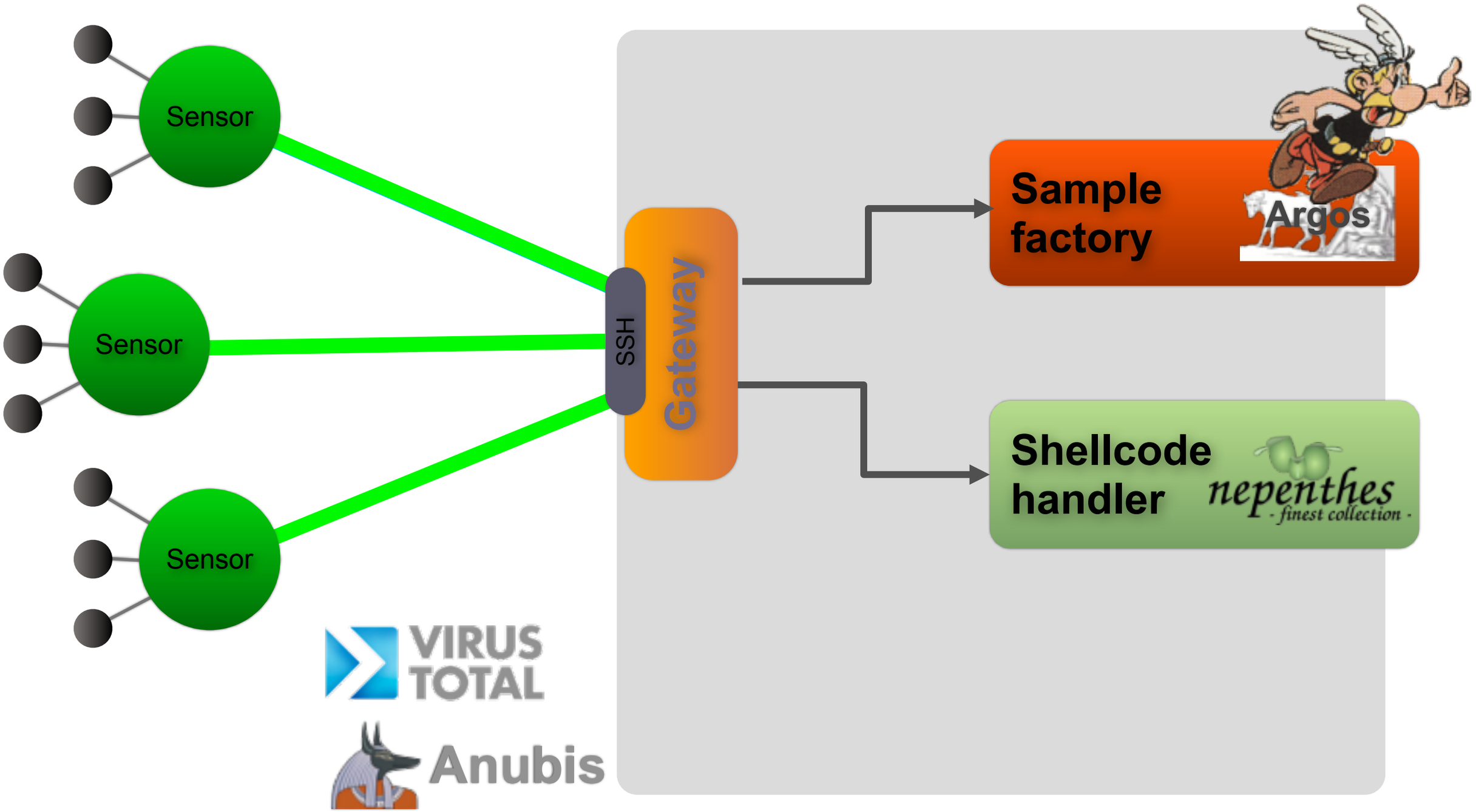
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



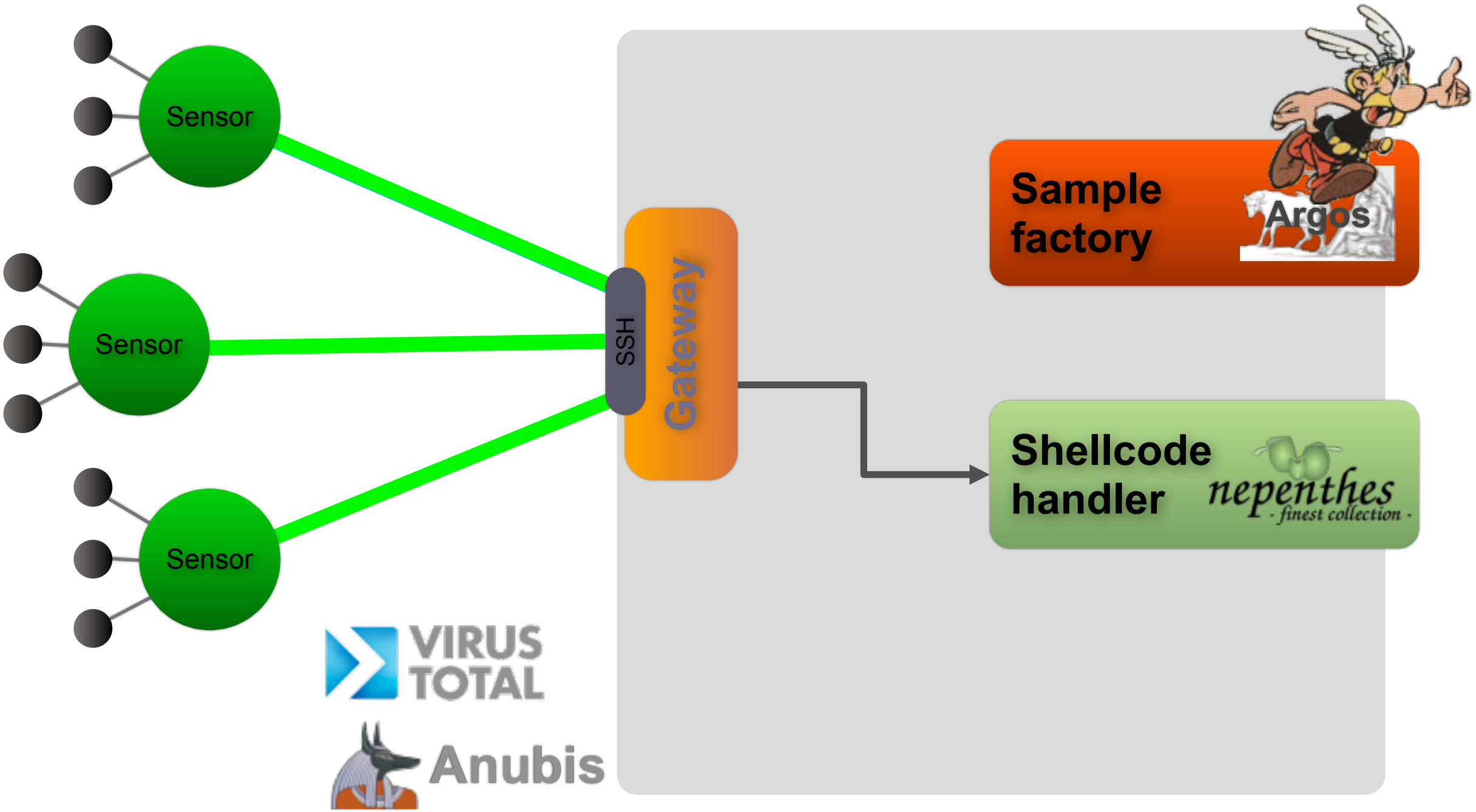
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



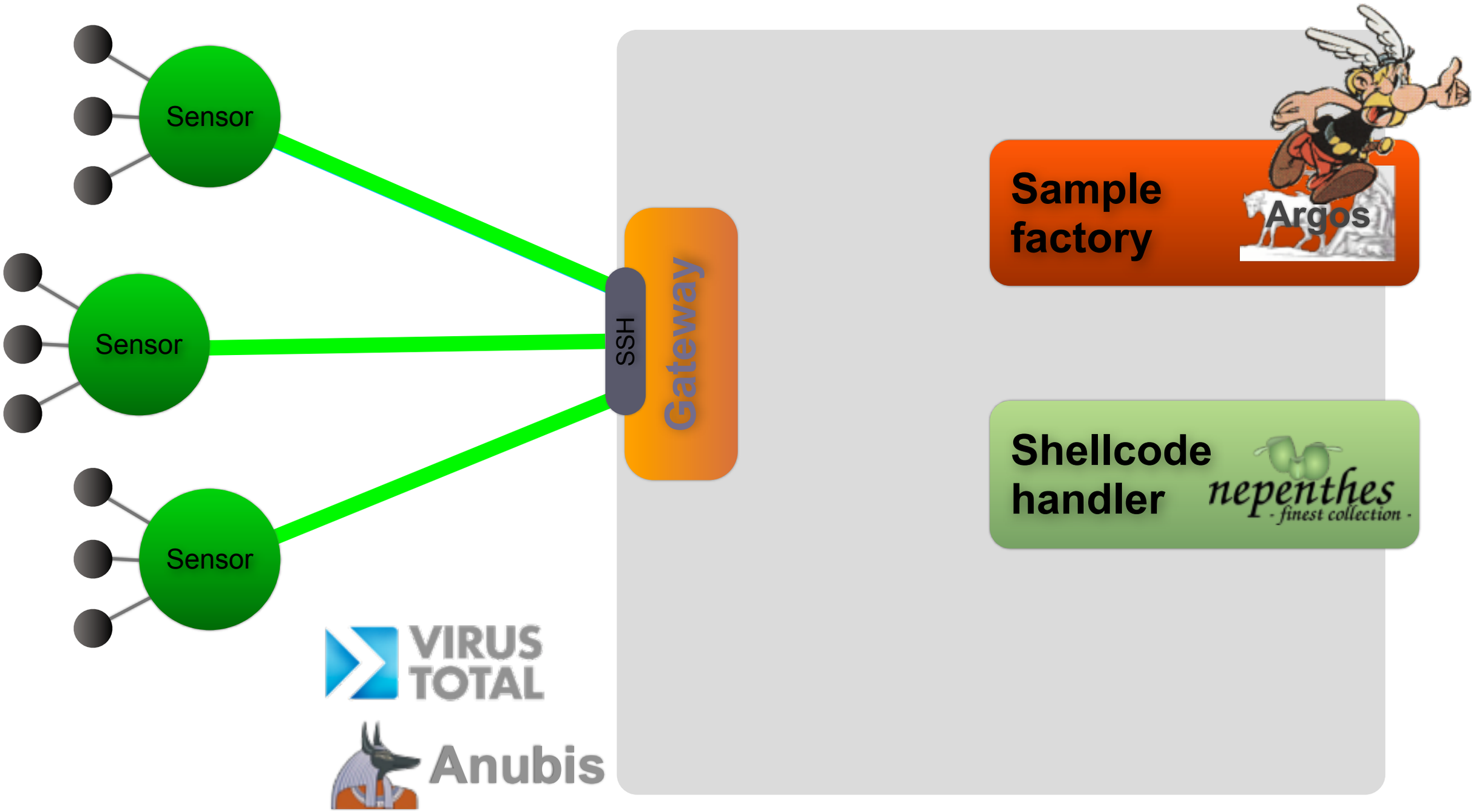
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



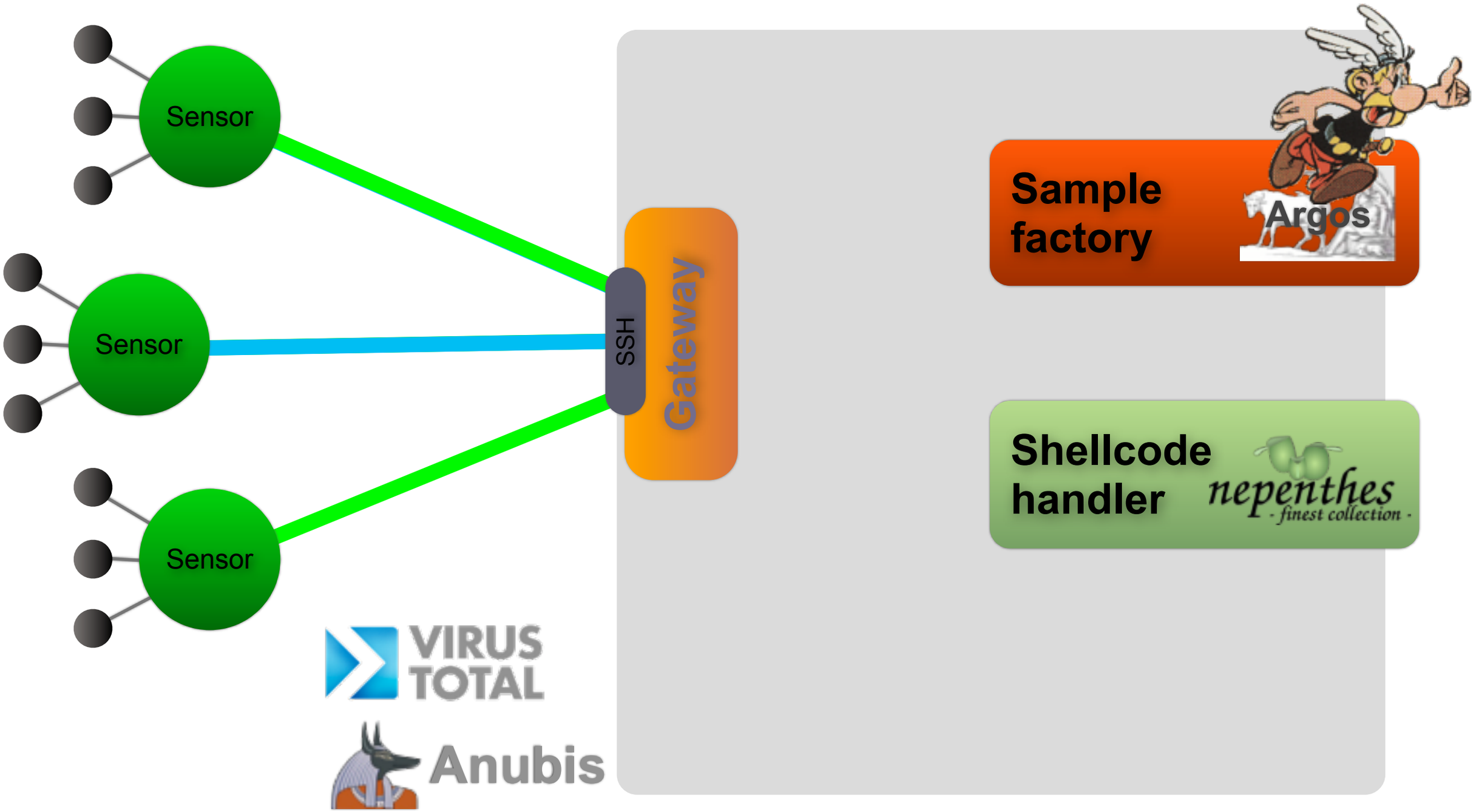
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



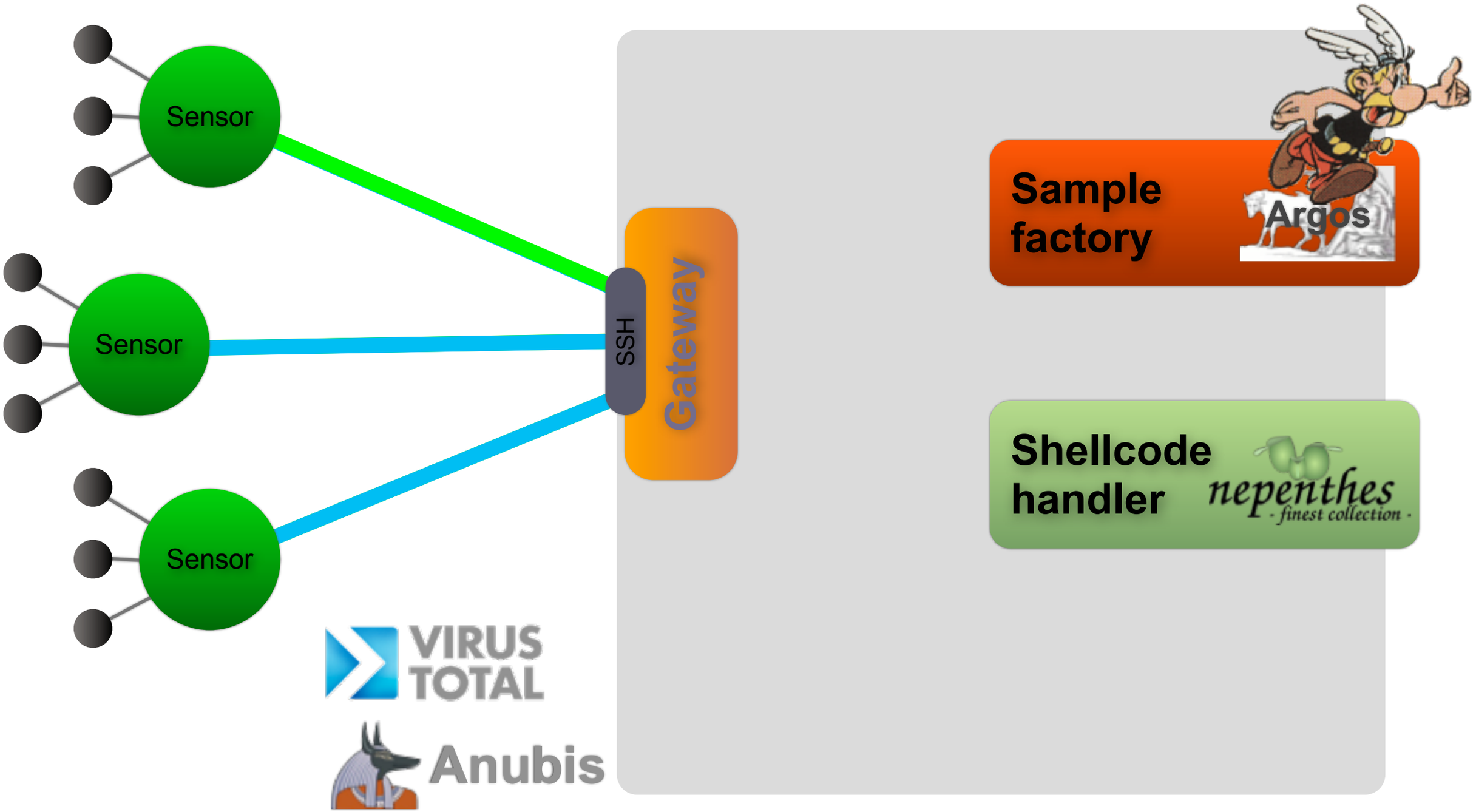
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



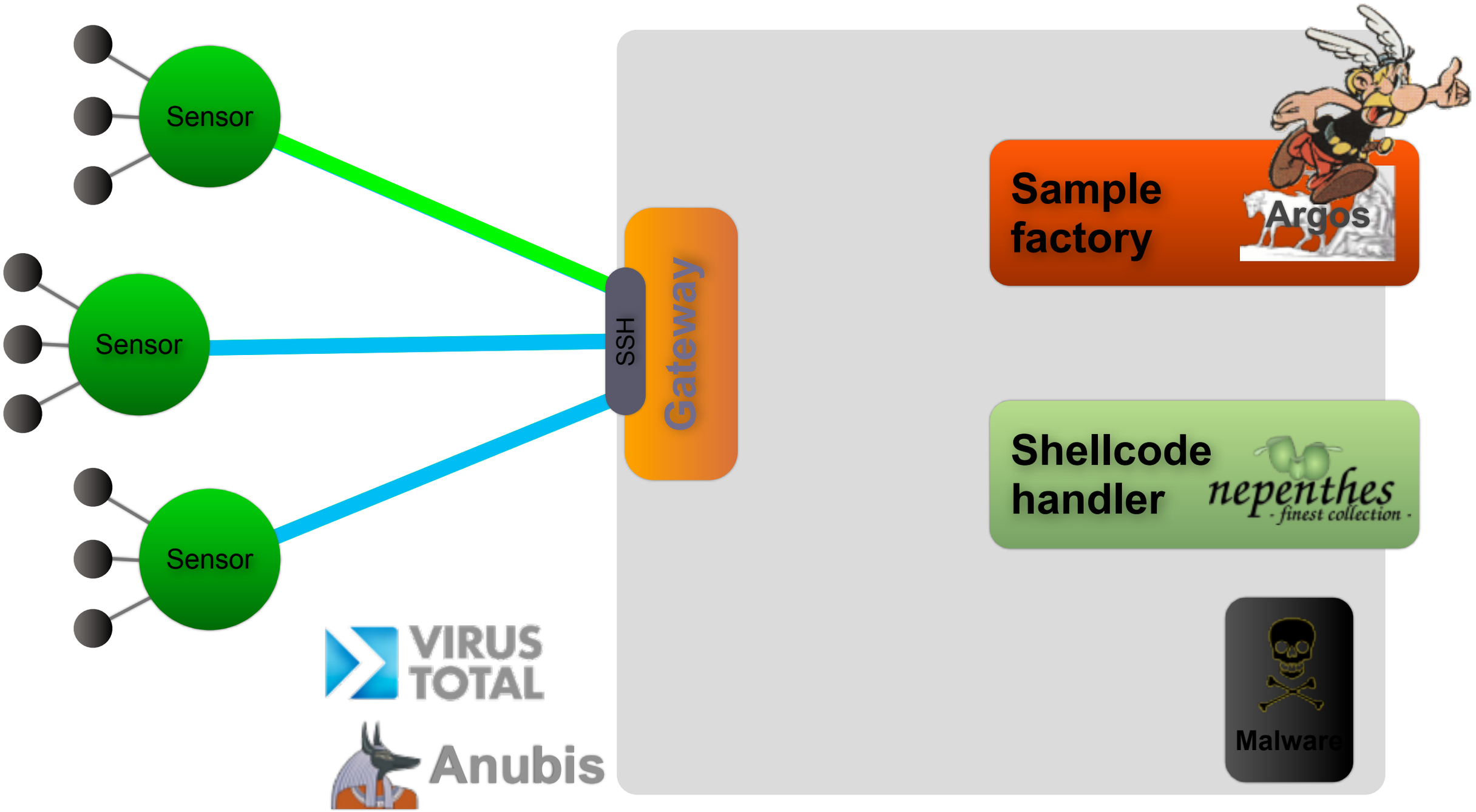
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



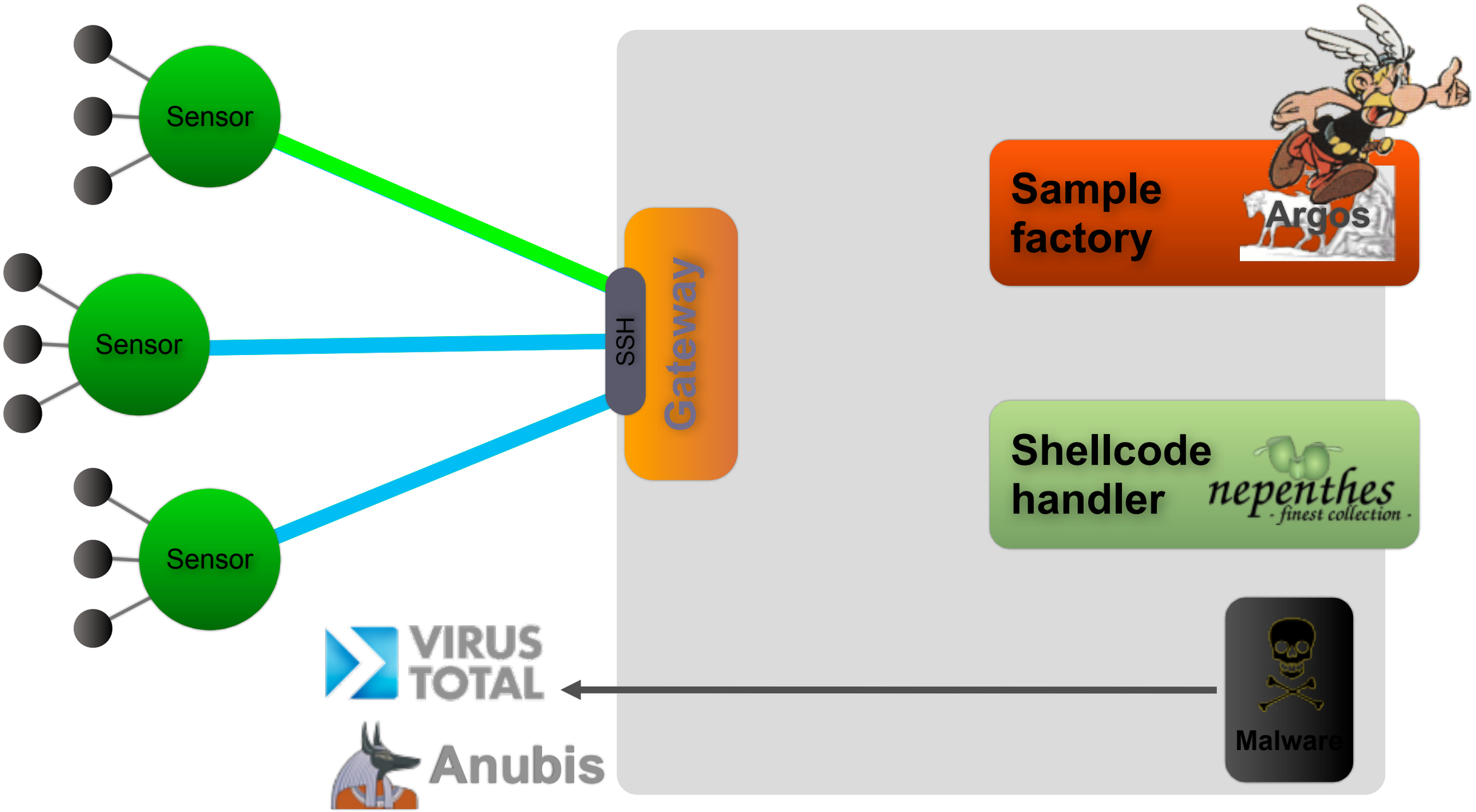
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



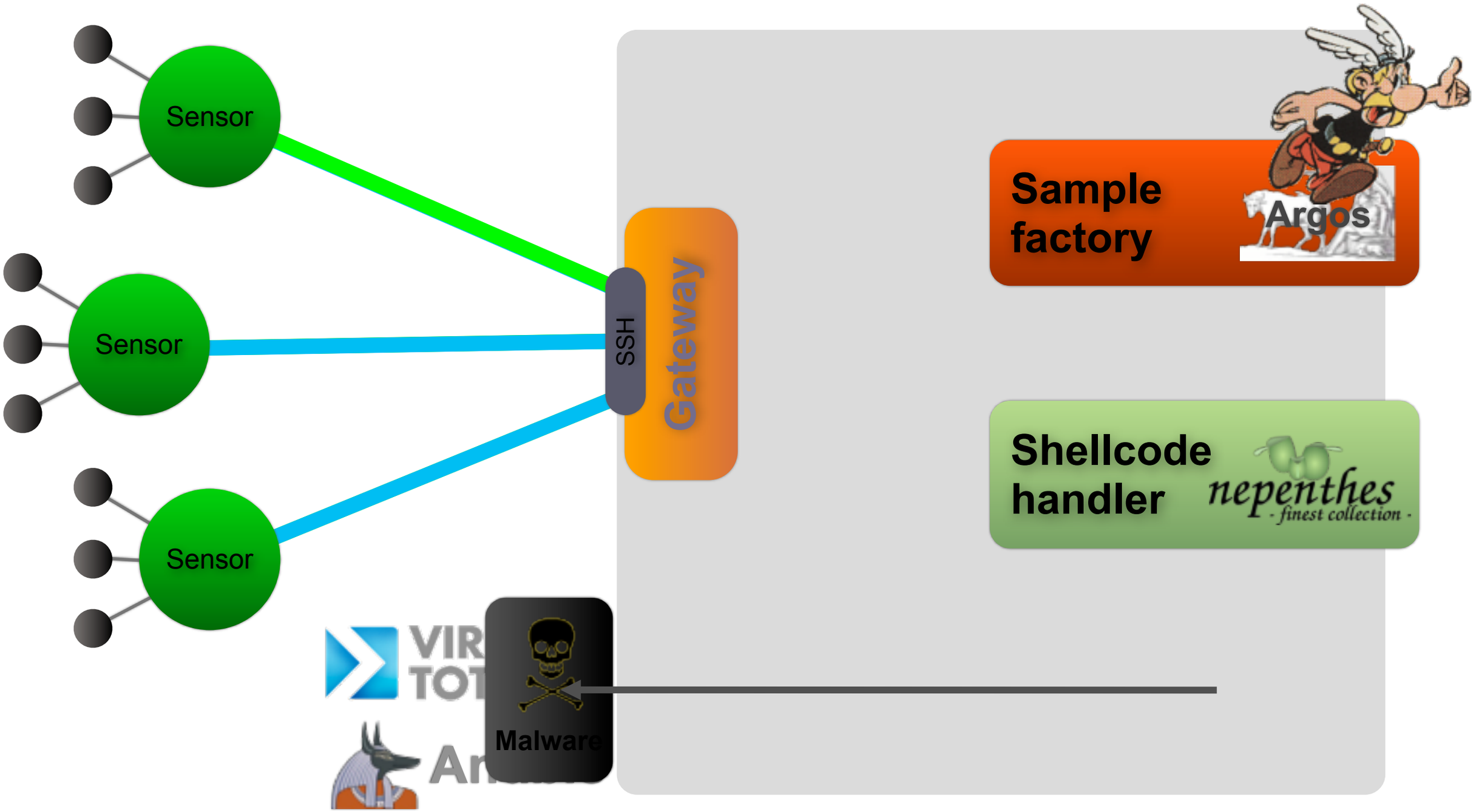
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



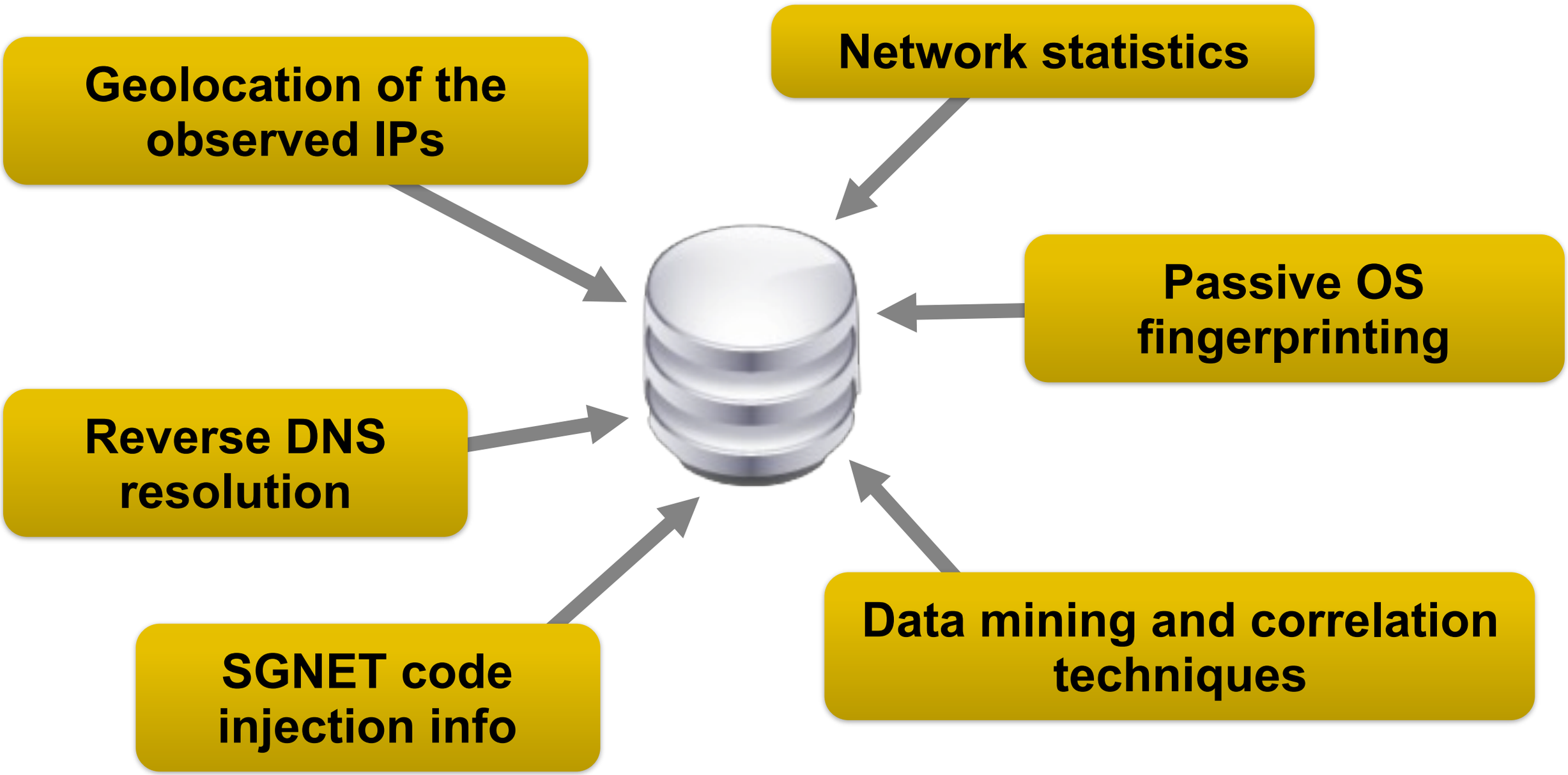
SGNE

- Normal operation
- New exploit encountered
- Global update of the FSM knowledge
- Submission of a shellcode sample
- Analyze new malware sample



Data enrichment

Data enrichment



VoIP honeypots

- Simulate PBXes, end-devices
  - e.g., Cisco phones, Nokia SIP-enabled cellphones, Android?

- Look for low-level vulnerabilities and misconfigurations
  - pre-requisite: analysis of common misconfigurations
  - challenge: how do we setup believable and trackable SIP honeypots?

Summary

- What we covered
  - VoIP protocols theory of operation
  - perceived threats against VoIP infrastructures
  - actual vulnerabilities in VoIP systems
  - Research being done
  - VAMPIRE project
- Availability threats are predominant
  - clients and servers equally vulnerable; little research being done
- Of the rest, weak/bad configurations and cross-protocol problems are the hardest to detect
  - often the most catastrophic as well
- How do we secure a complex infrastructure of this scale and complexity?