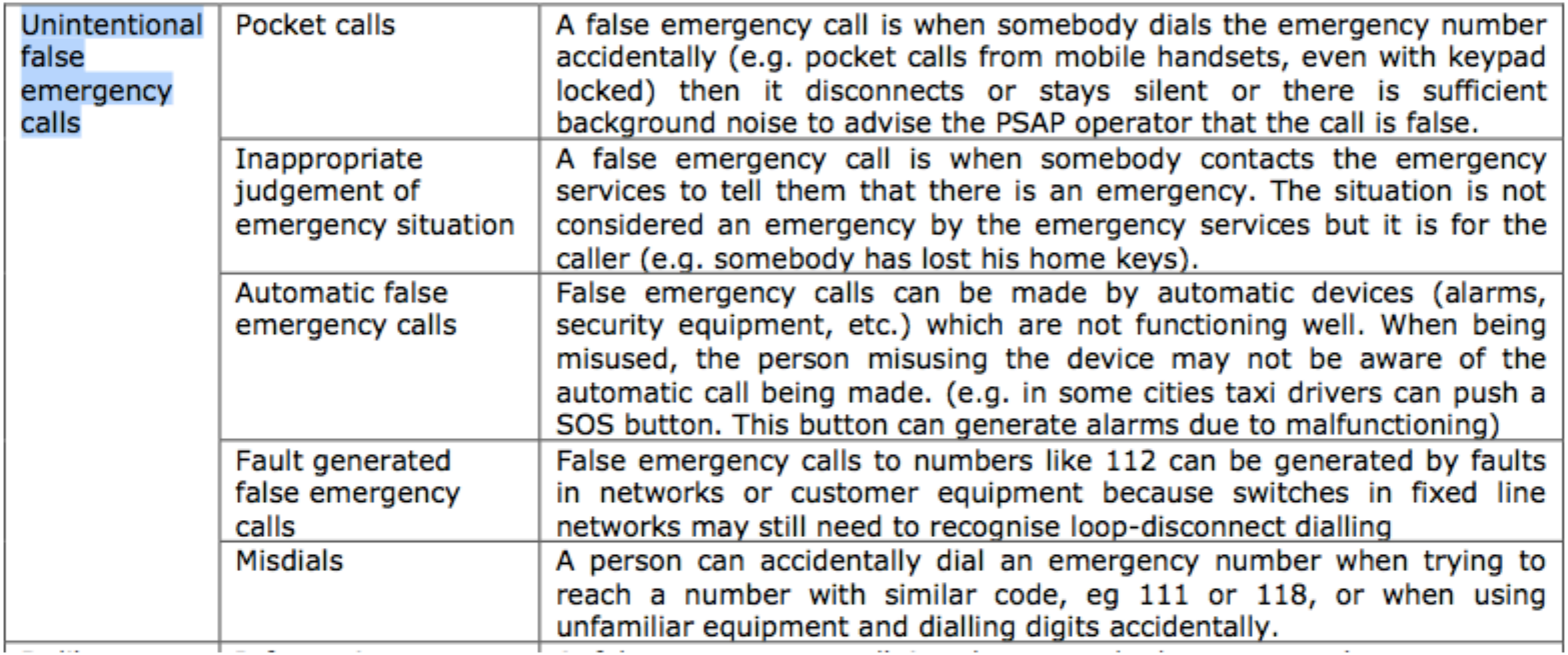
Risks with IP-based Emergency Services

draft-ietf-ecrit-trustworthy-location

Status

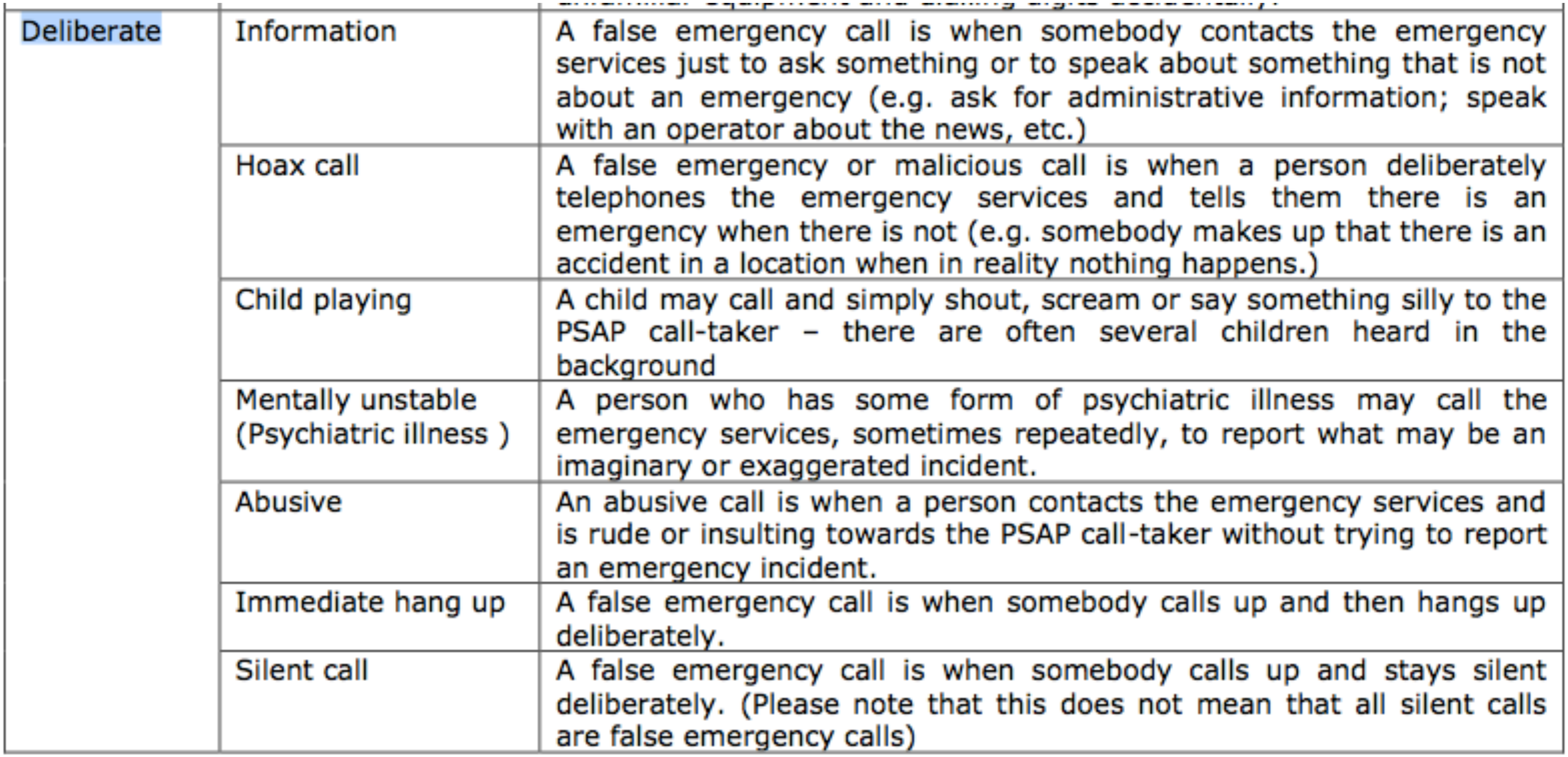
- Emergency services build on top of existing IP-based communication infrastructure.
  - As such, they inherit the security problems from the underlying infrastructure.
  - But many of the same security mechanisms are applicable as well.
- Most severe problems are related to a special form of distributed denial of service attacks:
  - EENA document tries to investigate "False Emergency Calls" in a more structured way: http://www.eena.org/ressource/static/files/2011_03_15_3.1.2.fc_v1.0.pdf
  - Swatting is a particular problem: http://www.fbi.gov/news/stories/2008/february/swatting020408
- draft-ietf-ecrit-trustworthy-location discusses these problems.
  - Views them from the angle of location (at least from the title although the text looks at it from a broader perspective).
  - But it does not offer a vision on how to deal with the problem.

False Calls



Unintentional false emergency calls	Pocket calls	A false emergency call is when somebody dials the emergency number accidentally (e.g. pocket calls from mobile handsets, even with keypad locked) then it disconnects or stays silent or there is sufficient background noise to advise the PSAP operator that the call is false.
	Inappropriate judgement of emergency situation	A false emergency call is when somebody contacts the emergency services to tell them that there is an emergency. The situation is not considered an emergency by the emergency services but it is for the caller (e.g. somebody has lost his home keys).
	Automatic false emergency calls	False emergency calls can be made by automatic devices (alarms, security equipment, etc.) which are not functioning well. When being misused, the person misusing the device may not be aware of the automatic call being made. (e.g. in some cities taxi drivers can push a SOS button. This button can generate alarms due to malfunctioning)
	Fault generated false emergency calls	False emergency calls to numbers like 112 can be generated by faults in networks or customer equipment because switches in fixed line networks may still need to recognise loop-disconnect dialling
	Misdials	A person can accidentally dial an emergency number when trying to reach a number with similar code, eg 111 or 118, or when using unfamiliar equipment and dialling digits accidentally.

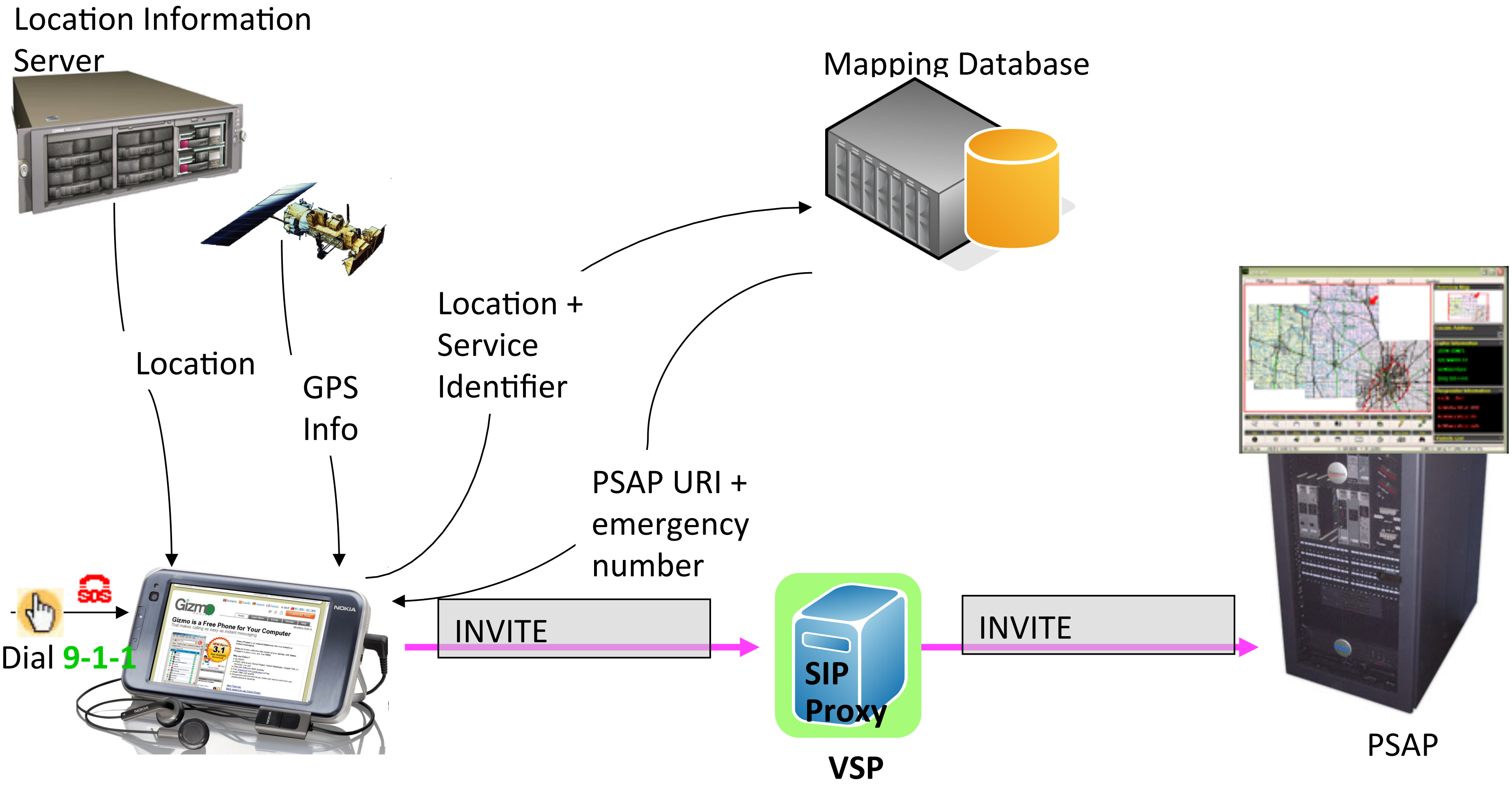
False Calls, cont.



		unfamiliar equipment and dialing digits accidentally.
Deliberate	Information	A false emergency call is when somebody contacts the emergency services just to ask something or to speak about something that is not about an emergency (e.g. ask for administrative information; speak with an operator about the news, etc.)
	Hoax call	A false emergency or malicious call is when a person deliberately telephones the emergency services and tells them there is an emergency when there is not (e.g. somebody makes up that there is an accident in a location when in reality nothing happens.)
	Child playing	A child may call and simply shout, scream or say something silly to the PSAP call-taker – there are often several children heard in the background
	Mentally unstable (Psychiatric illness)	A person who has some form of psychiatric illness may call the emergency services, sometimes repeatedly, to report what may be an imaginary or exaggerated incident.
	Abusive	An abusive call is when a person contacts the emergency services and is rude or insulting towards the PSAP call-taker without trying to report an emergency incident.
	Immediate hang up	A false emergency call is when somebody calls up and then hangs up deliberately.
	Silent call	A false emergency call is when somebody calls up and stays silent deliberately. (Please note that this does not mean that all silent calls are false emergency calls)

False Calls, cont.

- Number of reasons for false calls.
- Many of them cannot be “solved” via technical means!
- What is our story to deal with hoax calls/ swatting?
- Note: Problem is not unique to IP-based emergency services. Legacy networks also suffer from these problems.



Location Information Server

Mapping Database

Location

GPS Info

Location + Service Identifier

PSAP URI + emergency number

Dial 9-1-1

INVITE

SIP Proxy

VSP

INVITE

PSAP

The Attribution Problem*

- Attribution …
  - Requires to identify the agent responsible for the action
  - Determining the **identity or location of an attacker** (or an attacker's intermediary).
- Four aspects of attribution:
  - Types: if users are expected to be identified in some way, what is the source of that identity, and what can we conclude about the utility of different sorts of identity?
  - Timing: what are the different roles of attribution before, during and after an event?
  - Investigators: how might different parties exploit attribution as a part of deterrence?
  - Jurisdiction: what are the variations that we can expect across different jurisdictions, and how might this influence our choices in mechanism design?

(*) D. Clark, S. Landau, "Untangling Attribution", in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing, 2010.

Types of Identity

- Goal: real-world identity of the emergency caller
- Can only be obtained via resolution steps:
  - SIP AoR and resolution via VSP
  - IP address and resolution via ISP/IAP
  - Entirely independent mechanism (which does not yet exist, like emergency service certificates).
- Requires in-person identity proofing (and higher level of assurance infrastructure) during user registration.

Location

- Physical location of adversary may help PSAP call taker in decision making.
- Spoofable to a certain degree since the location configuration steps are vulnerable to manipulation.
- Assumes network provided location
  - Rules out many practical deployments.

Timing

- Before the Fact: Prevention or degradation
  - Example: Disallow SIM-less emergency calls
- Ongoing: Attribution as a Part of normal Activity
  - Example: Education about cost of emergency services infrastructure.
- During the Fact: Mitigation
  - Example: Signal 'false call' warning to caller.
- After the Fact: Retribution
  - Example: Take person to court.

Our Recommendations?

- Can we better describe solution possibilities and their challenges.
- Example challenges:
  - identity proofing is expensive
  - problems with different jurisdictions being involved
  - Traversing links from digital identity to real-world entity and physical location is difficult (and chain easily breaks)
  - Knowing the location of the adversary does not immediately lead to the real-world entity
- There are non-technical challenges and solutions as well.