Establishing trust in insecure distributed sensor networks

Alex.Perry@GE.com
GE Infrastructure, Security

Issues and solutions in securing the facility perimeter against a terrorism threat that may seek to compromise local communications.

imagination at work

Establishing trust in insecure distributed sensor networks
Outline

Why do we need to worry about trust ?

Should miniature sensors have any privacy ?

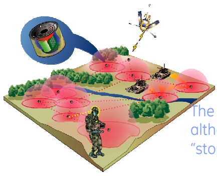
How do we characterize a sensor mesh ?

What methodology could manage all this ?

imagination at work

Good sensors want Trust, Privacy and a gossiping Social Community … ?

We want a magic wand to indicate dangerous people and explain why they need stopping.



The military needs it too, although their definition of "stop" is more permanent.

imagination at work

Why do sensor networks need trust ?

Making decisions with consequences

These are often irreversible – once made

Military: You cannot un-neutralize targets

Criminal: You cannot un-arrest someone

Civil: You cannot un-eject a customer

The decision is based on the data available

Without trusting data, how to decide ?

imagination at work

Without trust in data delivery, you couldn't believe the wand

Red light: Detected explosives, a gun or some other weapon.

Green light: Clear. Really. You know. *Of course* nobody modified anything. You can let him go now.

He's not the terrorist you're looking for

imagination at work

Similarities with Web Services

Finding a server using context and namespace

e.g. BIND9 and mandatory DNSSEC

Establishing a trusted path to that server

e.g. SSH with host public keys from DNS

Convincing the server to use our delivery

e.g. NGSCB shows real data was collected

Avoiding disclosure if device compromised

e.g. crypto libraries for persistent storage

imagination at work

Differences from Web Services

Hostile Denial Of Service – please try later

Has to be a deadline before one must act

Gossip about compromise – shop elsewhere

We can't simply stop providing security

Avoid malicious damage – use secured facility

That'd be a recursive suggestion, sorry

Website represents a company – so sue them

Sensors cannot sue monitoring station …

Why do sensor networks need privacy?

Sensors inspect humans … and their payloads

Much like a stateful firewall or similar

Validating oracles simplify breaking security

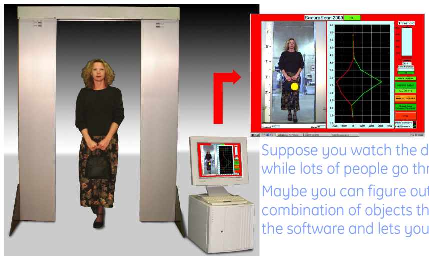
For network, document and human traffic

Need to avoid sensor results being accessible

Otherwise attackers can learn the sensor

Find out its limitations and avoid detection

Without sensor privacy, you shouldn't trust algorithms



Suppose you watch the data graph while lots of people go through.

Maybe you can figure out an special combination of objects that confuses the software and lets you through … ?

Similarities with Privacy Technologies

Restrict data payloads to specific recipients

e.g. Need to use asymmetric encryption

Describe distribution policy to the sensors

e.g. GnuPG's Web of Trust … as a tree

Distribute keys and signatures carefully

e.g. SSL tunnel to the key server (s)

Avoid side channel attacks on data flow

e.g. Pad short messages with noise

Differences from Privacy Technologies

Key revocation needs to be redistributed

Usually not the key issuer that revokes

Data is compromised after the effective date

This is real time, so retroactively discard

Data fusion combines from many sources

Tempting target, revoke and reprocess

Key manager is not co-located with the key

Use indirect signing by the managers

Circumvent being Examined …

Walk round/through when nobody is looking

Humans can be distracted by other events

Automatic visual tracking

Spoofing / countermeasures

Compare different methods

Explosive sensor:

Gun sensor:

Why do sensors need a community ?

Compare information about their vicinity

Dynamic distribution of picture streams

Identify occasional signature inconsistencies

Indicative of camouflaged humans ?

Identify consistent changes in conversation

Indicative of owned devices or sensors?

Notice suspicious changes in timestamps

Indicative of devices changing configuration

Take action outside Field of View …

Proceed behind columns or other people

Use multiple points of view and correlate

Compare track over sensors

Range ambiguity – scale errors

True 3D tracking cameras …

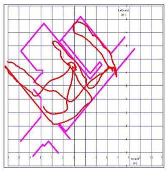
Visual:

Gun tracks:

Similarities with Online Communities

Rapid notification of run/stop state changes

Presence does this



Compare signatures

Pass documents

Hand off individuals

Use chat session

Each unit watches and tracks guns in one area

System manager can read/watch session

Zones with interlocking coverage

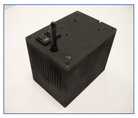
Battery operated wireless sensor arrays

Relocate to change interlock pattern

Analysis can learn …

Whose pattern?

Sub channel signals



Differences from Online Communities

Sensors cannot recognize a good community

There is no parental guidance available

Current online communities are not secure

In the sense of finding its members

Communities derived from the fields of view

Need a signature on the community

Summary

Sensors must autonomously find trusted paths

Their data delivery must remain inaccessible

The ways to combine data should be obscured

Tested, working components are out there …

Just put them together.

Any questions ?