Certificate-based, disruption-tolerant roaming architecture

Hideaki Goto  NII / Tohoku University
Outline

- Weakness of current authentication in eduroam
- Development of disaster-tolerant Wi-Fi system as a National Project after the Great East Japan Earthquake (2011)
  - DTN: Delay/disruption-tolerant network
  - DTN-AP stations & Portable DTN-APs
  - Certificate-based local AuthN mechanism
- Disruption-tolerant roaming architecture
  - Adaptation of DTN-AP system to eduroam
  - Combined with eduroam Delegate Authentication System (DEAS)
eduroam architecture

- Various EAP methods such as PEAP, EAP-TTLS
- Based on *relaying AuthN requests* (except RadSec)
- IDPs and proxies need to be alive always!
Weakness of the current architecture

- Unstable, slow user authentication, sudden disconnections, etc.
  - Many hops of AuthN requests
  - Long-haul communications across continents
  - Congestion of proxies / networks
- Vulnerable to network/proxy failures
  - Temporary network disruptions
  - Hardware malfunctions
  - Software glitches
  - Configuration errors
  - Power loss, etc.
Disruption-tolerant eduroam – an idea

- Tolerant of temporary server / proxy / network failures
- Efficient, fast and reliable AuthN
- Compatible with current eduroam (no modification on the core architecture)
- Just an add-on
- Can be deployed partially and gradually
- Would contribute to public Wi-Fi systems under natural disasters
DEAS: Delegate Authentication System

- Centralized eduroam IdP
  - simplify eduroam deployment work
  - simplify the RADIUS proxy tree for higher stability
- Web service as an eduroam account issuer
- 3 types depending on the needs and federation level
- Account Issuer as a Shibboleth SP of Japan’s GakuNin federation (optional)

Just sign-up to join eduroam!
DEAS simplifies the AuthN network

- Large RADIUS tree can be replaced with a single RADIUS server which works as an IdP for member institutions.

RADIUS tree of the basic eduroam

Centralized RADIUS server of DEAS

User@instD.jp

DEAS

IdP

no fed. or Shibboleth
3.11 The Great East Japan Earthquake

March 11, 2011

14:46 The main quake of **M9.0**
15:08 aftershock of **M7.5**
   (off the Sanriku coast)
15:15 aftershock of **M7.3**
   (off the coast of Ibaraki pref.)
15:25 aftershock of **M7.4**
   (at the Japan Trench)

Tohoku University Research Center for Prediction of Earthquakes and Volcanic Eruptions, Assistant Prof. Uchida
http://www.aob.geophys.tohoku.ac.jp/info/topics/20110311_news/index.html
What happened on 3.11 and afterwards?

- A lot of residents and stranded people went to the near-by shelters and stayed there for some nights. (Shelters: schools, universities, government facilities, stations, company buildings, etc.)
- No electricity, no gas, not enough food/water
- Mobile networks were put into emergency mode, became heavily congested and almost unavailable all over the country.
- Almost no public Wi-Fi was available at the shelters.
- Quite limited communication means for citizens. (No public Wi-Fi at many shelters)
What are needed?

*People suffered from the shortage of information!*

- Communication means for rescue operations
- Communication means for staff of municipal governments and volunteers
- Local broadcast system and bulletin boards
- Communication supports such as public Wi-Fi for citizens’ terminals (smart phones, etc.), particularly at shelters
- Internet access has been found quite useful and important in disaster-affected areas.
Development of disaster-tolerant public Wi-Fi

- Following the experiences in the 311 Great Earthquake in 2011
- National Project funded by the Ministry of Internal Affairs and Communications (MIC)
  - Disaster- and fault-tolerant public Wi-Fi to help people under natural disasters, etc. (besides 3G/4G mobile networks)
  - Improving the effective Wi-Fi capacity at shelters for emergency cases
Our approach

- Based on the eduroam technology, i.e. roaming by 1X-based AuthN
- Priority control, broadcasts, access control, throttling, etc., using OpenFlow
  - Use the enhanced authorization mechanism
  - Add some special features for emergency use
- AuthN/AuthZ tolerant of partial disconnections of the network (incl. proxy failures)
Local AuthN for disconnected network

- The RADIUS network may be down.
  - Home institution is affected by a disaster.
  - IdP power loss, malfunction, etc.
  - Proxies on the path may be down.
Portable DTN Access Points

- DTN: Delay/disruption-tolerant network
- Equipped with Wi-Fi APs, local web server, storage, GPS, backup batteries

[Copyrighted material has been removed.]
Test-bed system with DTN-AP stations

- A test-bed system was built in the downtown of Sendai city. Each station consists of APs, local web server, storage, swappable backup batteries, and solar panel.
- Work as normal public Wi-Fi spots when the Internet is available.
- Turn into information repositories when the network is disrupted.
Certificate-based local authentication for DTN-APs

- EAP-TLS for client authentication

Signature verification for authentication
User attributes for authorization

Issuer's private key

Client certificate
Issuer
User name
Certificate
User attributes
Signature

Site A
LAN
DTN-AP A
RADIUS

Site B
LAN
DTN-AP B
RADIUS

EAP-TLS for client authentication
Key distribution and CRL handling in DTN-AP system

- Edge proxies need to have all issuers’ keys.
  - Prefectural governments are in charge of account issue.
  - Domestic system – 47 prefectures in Japan
- CRL cannot be retrieved when the network is down.
  - CRL caching for normal operations.
- Don’t care abuses so much. That’s under a disaster!
Disruption-tolerant eduroam architecture

- DEAS at each country works as the account issuer and provides the public key. (# of keys = at most 200)
- *Path A* is taken when the national server has the valid key cached.
- *Path B* is taken when the key is not provided. (fall-back)
- Every institution should have the public key of their country to make the most of the local AuthN mechanism.
Conclusions

- Disruption-tolerant eduroam can be realized by combining DEAS (or another), EAP-TLS, and public key/CRL exchange and caching mechanisms.
- Proof-of-concept system is available as DTN-AP. The development of a test-bed is under way.

Future work

- Performance measurements and analysis
  - How does the bigger packet of EAP-TLS affect to the performance and stability?