Stateless Architecture: for Security Innovation

Tim Mather
CISO and VP of Security & Compliance Markets, Splunk

Chenxi Wang, Ph.D.
Vice President, Principal Analyst, Forrester

Session ID: SECT-R35B
Session Classification: Intermediate
In South Africa, insurance companies can now underwrite policies for remote farmers using mobile phone photos of crops.
In Kenya, M-Pesa is used by 9 million customers (40% of adult population), and facilitates 10% of the country’s annualized GDP.
In the United States, physical car keys are becoming obsolete – replaced by mobile phone applications.
The Traditional Model is Broken

► Business model has changed
  ► No longer “all employee” – now includes contractors, partners, vendors
  ► No longer all “on premise” – now ‘everywhere’ and anywhere

► Data model has changed
  ► No longer strictly structured (e.g., transactional) – now largely unstructured

► Platform model has changed
  ► No longer strictly enterprise (e.g., mainframe, client / server) – now includes mobile, cloud, big data platforms
Trends Impacting the Model

► Increased connectivity requirements
  ► Increased demand for constant communications, combined with increasing adoption and use of mobile
  ► Pushing development of ad-hoc networks, cognitive radio

► Continued growth of BYOD
  ► Access and use of data that must be protected across:
    ► Locations, legal entities, and personnel
    ► Platforms and networks

► All of this is driving a stateless architecture
‘Traditional’ cell towers give way to femtocells
Feature phones give way to smart phones
Ongoing failures of traditional “state-dependent” data protection architectures

- Dissolution of “known” endpoints
- Failure of “behind-the-firewall” trust model
- Network-dependent measures simply not sufficient

Forcing a transition from network- and host-level protection to data-level protection models

- ‘Perimeter’ is now on the data-level itself
What it Means to have Stateless Security

- Controls are decoupled from the infrastructure
  - Data protection “travels” with the data
  - Independent of an application, network or device
- Trust is dynamic, on-demand
  - Trust is NEVER assumed
  - Trust is ALWAYS assessed at the point of access, dynamically
- Leverage on ecosystem capabilities by default
  - Rather than built in house
Four Steps of Building Stateless Architecture

► Leverage ecosystem capabilities
  ► Cloud services and cloud APIs
  ► Mobile APIs & libraries
  ► Security function as a service

► Build a middleware to extend your enterprise applications

► Exercise real-time threat and risk assessment

► Build protection into application, closer to data
An Example of Stateless Security Architecture

- Device reputation
- Commercial IdP
- Middleware: Access management, threat assessment, logging/auditing
- Core biz logic
- Security policies & functions
- Providing business services
- Fraud management
- Analytics

Core biz logic

Security policies & functions
An Example of Stateless Identity Management

1. Resource owner (user) accesses the service.
2. Resource owner (user) accesses the service.
3. Resource owner (user) authenticates, then grants access authorization.
4. Authorization server (STS) issues the access token (may refresh it later).
5. Resource server (web app) accesses the protected resource.

(in the same security domain)

Client (web app)

Authorization server (STS)
An Example of Stateless Security Control

Policy bits = high water mark*

2724 Ak8W Bn3M 2838

0012 3456 7890 0000

Original Data

Encrypted string

* The embedded Format-preserving encryption example came from Voltage Security
What it means

Security controls are enforced – without you having to own the full stack yourself

Security ecosystem delivers value far beyond traditional behind-the-firewall controls – powerful, contextual, immediate

More agile and rapid protection – infrastructure can change without rebuilding protection
Key Benefits

► Agile, rapid and efficient protection
  ► Data is protected regardless where they are

► Simple, modular and portable
  ► Infrastructure can change without rebuilding protection

► Reduce the trusted computing base (TCB)
  ► The “holy grail” of security
Thank you!