What my friends think I do

What my parents think I do

What I actually do
Deploying Uptane Onto Production Infrastructure

SOUTHWEST RESEARCH INSTITUTE

Allen Cain, Research Analyst
Embedded Systems Security Group
Intelligent Systems Division
Disclaimer

Any tools or technologies mentioned here are meant solely as a reference and are not intended to be an endorsement or preference by Southwest Research Institute.
Southwest Research Institute (SwRI)

- San Antonio, TX
- Non-Profit R&D
- Various Projects and Clients
- OTA Updates

Benefiting government, industry and the public through innovative science and technology.
OTA Updates

- Code Signing
  - NIST White Paper
  - Key Threshold
  - Key Rotation
  - Key Revocation
  - Key Placement
    • DevOps Integration

- Uptane

---

https://medium.com/@neonrocket/devops-is-a-culture-not-a-role-be1bed149b0
Uptane

- DHS Funded
- UMTRI, NYU, SwRI
- Includes Automotive Stakeholders

- Differences:
  - Multiple Repositories
    - Supplier Interaction
  - Multiple Keys
  - Offline Keys
  - Key Hierarchy
    - Assist Key Revocation/Rotation
Uptane – SwRI Responsibility

- Involved since Design and Requirements
- Responsible for Penetration Testing
  - SAE World Congress
- Threat Assessment Document
- Development of C-client
- Development of Back-End in Golang
Uptane – Outside Scope

▪ Right to Repair

▪ Dealer Interaction

▪ Call Center / Back-End Functions

▪ Web/Mobile Application

▪ Cloud Deployment
Moving to the Cloud

WHAT IF I TOLD YOU
THERE IS NO CLOUD. IT'S JUST SOMEONE ELSE’S COMPUTER.
Deploying Uptane

- **Cloud**
  - Someone Else’s Servers
  - Disaster Recovery
  - Physical Security
  - Efficiency
  - Scalability

- **Uptane on the Cloud?**
  - Offline
  - Online
    - Environment Variables
    - AWS CloudHSM
      - $12.7k - $18.2k a year

Supplier
Deploying Uptane

- **Cloud Tools**
  - Infrastructure-as-Code
    - Easy Provision and Management
    - Good Concept, Potential Risk

- **AWS Credentials**
  - Necessity?
  - Storage?
  - Multi-Factor Authentication
    - Software or Hardware
Deploying Uptane

- Managing Secrets
  - Hardcoded
  - Environment Variables
  - Configuration File
  - Amazon Secrets Manager
    - Built-in Secret Rotation

https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

```sql
// Connect to Uptane MySQL DB on AWS
database.DBCon, err = sql.Open("mysql",
    "UserName:Password@tcp(uptane-inventory-database.ceccowef7shh.us-east-2.rds.amazonaws.com:3306)/inventory_database")
```
Attacking the Cloud
Attacking Uptane

- Cloud Issues
  - Default Configurations
    - Cryptojacking
  - S3 Misconfiguration
    - Unauthorized List, Download, Upload
  - Lack of Separation of Privilege
    - Utilize IAM Roles
  - API DOS
    - Utilize Amazon API Gateway
  - Insufficient Logging
    - Amazon CloudWatch

https://blog.redlock.io/cryptojacking-tesla
Attacking Uptane

- Cloud is Growing
  - Data Centers in New Regions
  - Cloud HSM
  - AWS Secrets Manager
  - Amazon FreeRTOS
  - AWS Marketplace
    - Charlie Miller
    - Janus

New Android vulnerability allows attackers to modify apps without affecting their signatures
Next Steps

- Best Practices
  - Principle of Least Privilege
  - Enable Logging w/ Alerts
  - Defense in Depth
  - Deploy in Multiple Regions
  - Treat Everything as Untrusted
  - Penetration Testing
  - Security Training
  - Integrate Security into DevOps

https://www.sans.org/security-resources/posters/secure-devops-toolchain-swat-checklist/60/download
Next Steps

- Performing Code Signing
  - Uptane
- Cloud Provision and Management Tools
- Cloud Security
In Conclusion
Questions?

Allen Cain
Research Analyst
Embedded Systems Security
Allen.Cain@swri.org