Welcome to the Allegion Custom Keys Session!

Using your phone, tablet or laptop, type this in your browser:

www.menti.com

Enter this code:

33 24 64
University-Owned Keys: How Your Colleagues Are Finding Freedom Through Smart Card Interoperability

April 4, 2017

David Stallsmith - National Account Manager, Allegion
Jeff Vonderschmidt - Manager Systems & Development, Indiana University
Agenda

- Contactless cards overview
- What are smart cards?
- Why smart cards are good
- How smart cards work with our existing infrastructure
- Will owning our encryption keys future-proof our card system?
- How Indiana University is doing it
- Phones and IDs
Presentation gadget

Using your phone, tablet or laptop, type this in your browser:

www.menti.com

Enter this code:

33 24 64
Prox is bad; smart is smart

Contactless Smart Card Overview
Prox technology

Good:
- Long read range
- Existing infrastructure

Bad:
- 30 years old
- Very easy to clone a prox card
- Prox card formats do not provide security anymore
Smart cards

Why they’re better than prox

- Encryption!
  - Nobody can copy your card

- Extra data storage for other applications
  - Other systems
  - Offline locks
  - Transit

Breach
Putting smart card encryption into perspective:

Sniffing, Brute Force & Replay Attacks
Encryption Key Perspective

Brute force attack scenario

- AES 128-bit encryption
- AES 256-bit encryption
AES-128

$340,282,366,920,938,463,463,374,607,431,768,211,456 \times 2 = 680,564,733,841,876,926,926,749,214,863,536,422,912$

$2^{129} \neq 256$-bit
115,792,089,237,316,195,423,570,985,008,687,907,853,269,
984,665,640,564,039,457,584,007,913,129,639,936

grains of sand in Sahara Desert
ounces of water on Earth
atoms in quattuorvigintillio
n atoms on
Brute force attacks

AES 128-bit encryption

- Fastest super computer: 10.51 petaflops (10.51 x 10^{15} operations / second)
- Operations required per combination check: 1,000 (optimistic, assume for now)
- Combination guesses / second = (10.51 x 10^{15}) / 1000 = 10.51 x 10^{12}
- Seconds in one year = 31,536,000
- Years to crack AES with 128-bit Key = (3.4 x 10^{38}) / [(10.51 x 10^{12}) x 31536000] = 1,020,000,000,000,000,000,000,000 years (billion billion)
The security of smart technology

- **Smart Technology**
  - The card and reader communicate back and forth
  - Each verifies that the other is legitimate

- **Mutual authentication**
  - Each verifies that the other is legitimate

- **Encryption**
  - Card and reader communicate in “secret code”
  - An algorithm prevents the ability to discern the communication

- **Key diversification**
  - Each card has a unique key
  - Prevents compromise of the entire population

---

13 | University-Owned Keys
How to play well with others

Compatibility
Smart cards and system compatibility

What has to line up

- Chips
  - Card and reader

- Card formats
  - Card, reader, system

- Encryption
  - Algorithm
  - Key

Incompatibility
NXP smart card chips
University-owned keys!

- **Encryption key**
  - Created by Allegion
  - Created by university

- **Owned by the university**
  - Held by Allegion
  - Shared with the university
Advantages

- **Security**
  - Attack on manufacturer’s standard key does not affect university key

- **Interoperability**
  - University can share their key with vendors
  - Puts the university in the driver’s seat for security system component selection
How’s it going at IU?

Heeeeere’s Jeff!
Indiana University

Locations and options

<table>
<thead>
<tr>
<th>IU Campuses</th>
<th>IU School of Medicine Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overseas Study Programs</th>
<th>Classes, Approximately, Offered Each Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>350+</td>
<td>20,000</td>
</tr>
</tbody>
</table>

Employees

<table>
<thead>
<tr>
<th>Faculty, Staff, and Other Employees as of Fall 2015 (Excluding IPFW)</th>
<th>Countries Represented by IU Faculty</th>
</tr>
</thead>
<tbody>
<tr>
<td>19,000+</td>
<td>120+</td>
</tr>
</tbody>
</table>

20 | University-Owned Keys
The IU Class of 2016

These numbers exclude IPFW, which IU does not administer.

19,477 graduates
27% are first-generation students
18–71 age range of graduates

Our students, as of fall 2015

114,000+ students university-wide
78,000+ degree-seeking undergraduate students
19,000+ students in graduate and professional programs

72% of degree-seeking students are Indiana residents
8,700+ international students from 130+ countries
22% of domestic, degree-seeking students are multiracial, African American, American Indian, Asian American, Hispanic, or Pacific Islander (excluding IPFW)

Alumni

650,000+ living graduates worldwide
160+ alumni communities worldwide
Don’t just call me…
Phones

Phones to open doors
Phones and physical access

How can a phone communicate with a reader?

- Card emulation (NFC, BLE)
  - Phone acts like card
  - No network required
  - Cost per mobile credential
- iPhone vs. Android
  - NFC and BLE
Phones for access now?

- Phone-reader compatibility
- Support
- Early days of development of mobile for access control
  - Access control system providers are developing their own apps
  - CBORD, Kastle

End of the badge? These smart doors will open for you.
What should we do?

Assess risk
- Physical access
- Payments
- Don’t just survey how comfortable everyone feels now

Assess existing infrastructure
- How many readers?
  - Locks
  - Payment terminals
- Other systems to interface?
- Transit system integration
Consider an upgrade to cards and readers

What is supported by my card system?

- How will we issue credentials?
- Will we have to replace readers and terminals?

Should we wait for mobile?

- “Intent” still being worked out
- Wait for more mature solutions that include cards

What would it take?
NXP smart card chips

- Supported by the most manufacturers
- Widest range of options
- Most applications worldwide
- Common Criteria certified EAL4+/5+

Own your smart card encryption key!
Thanks!
Contact Us - Add photos if possible

David Stallsmith
National Account Manager
Allegion
704-351-0466
David.Stallsmith@allegion.com

Jeff Vonderschmidt
Manager Systems & Development
Indiana University - Bloomington
812-855-4330
jvonders@iu.edu
Indiana University and Smart Cards

What they did at IU
IU has their own custom key
- Why IU wanted the additional security of a custom key
- Flexibility in choosing providers
Group Questions

Why don’t you use phone credentials for access and payments now?
- Expense
- Too hard – politics, no time, don’t know how, I hate phones
- Don’t lead

How much would you pay for phone credentials?
Be honest, please
- $10+
- $6-10
- If a smart card costs $3-5,
- If you could issue only a mobile credential
- When will schools move away from plastic and why?

Q: What system would you use your card/phone for?
Q: What are they waiting for?