Secure Coding Practices in Java: Challenges and Vulnerabilities

NA MENG
STEFAN NAGY
DANFENG (DAPHNE) YAO
WENJIE ZHUANG
GUSTAVO ARANGO ARGOTY

VIRGINIA TECH

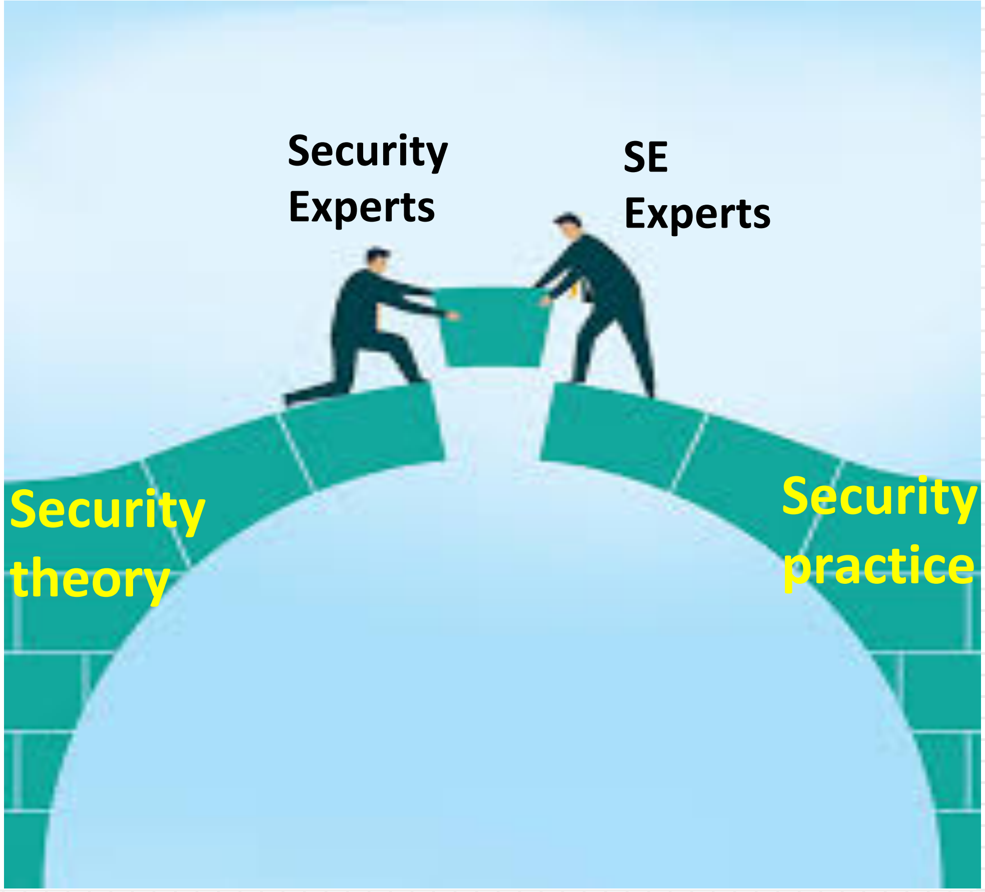
Problem Statement

- Security libraries facilitate secure coding
  - E.g., APIs for cryptography, SSL, and authentication
- Library misuses cost lots of debugging effort, and cause security software vulnerabilities

Related Work

- Cryptographic vulnerabilities and misuses [Lazar et al. 2014, Nadi et al. 2016]
- SSL misuse and man-in-the-middle (MITM) attack [Fahl et al. 2012, Georgiev et al. 2012]
- Vulnerabilities in Android code [Acar et al. 2016]

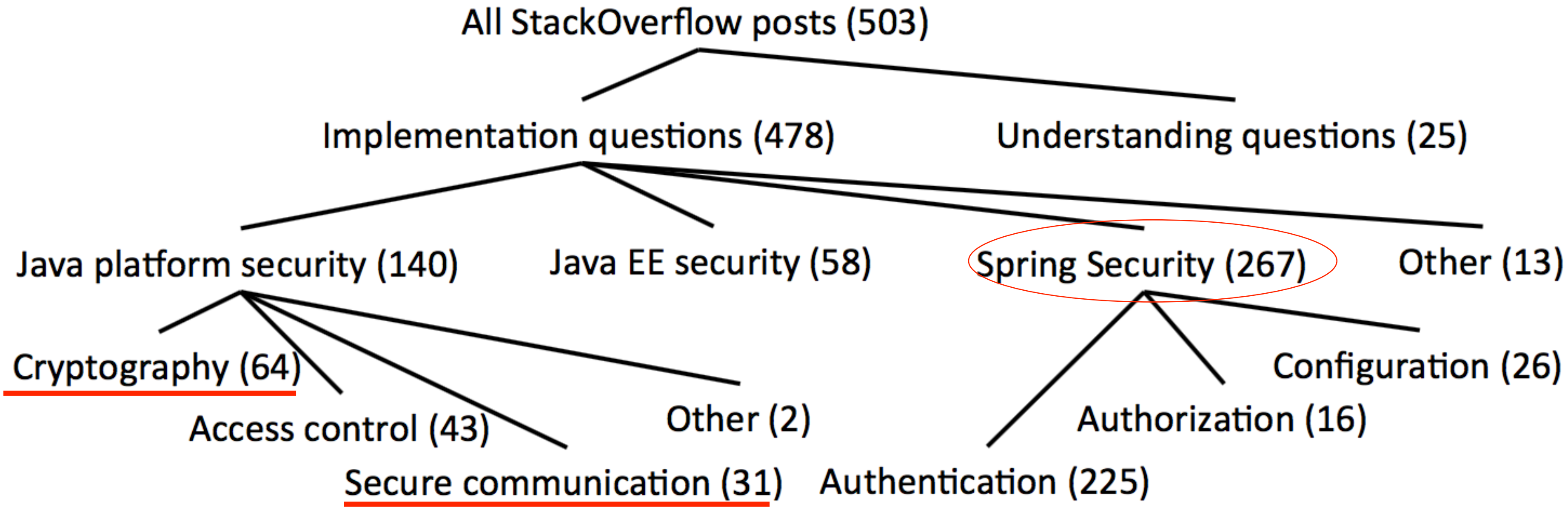
What are the biggest challenges and vulnerabilities in secure coding practice?



Methodology

- 22,195 StackOverflow (SO) posts containing keywords “Java” and “security”
- Mainly focus on 503 posts for manual inspection after filtering the posts
  - Initially classify posts based on the software libraries under discussion
  - Further refine the classification based on the security concerns, e.g., cryptography, access control

RQ1: What are the common concerns?



All StackOverflow posts (503)

Implementation questions (478)

Understanding questions (25)

Java platform security (140)

Java EE security (58)

Spring Security (267)

Other (13)

Cryptography (64)

Access control (43)

Secure communication (31)

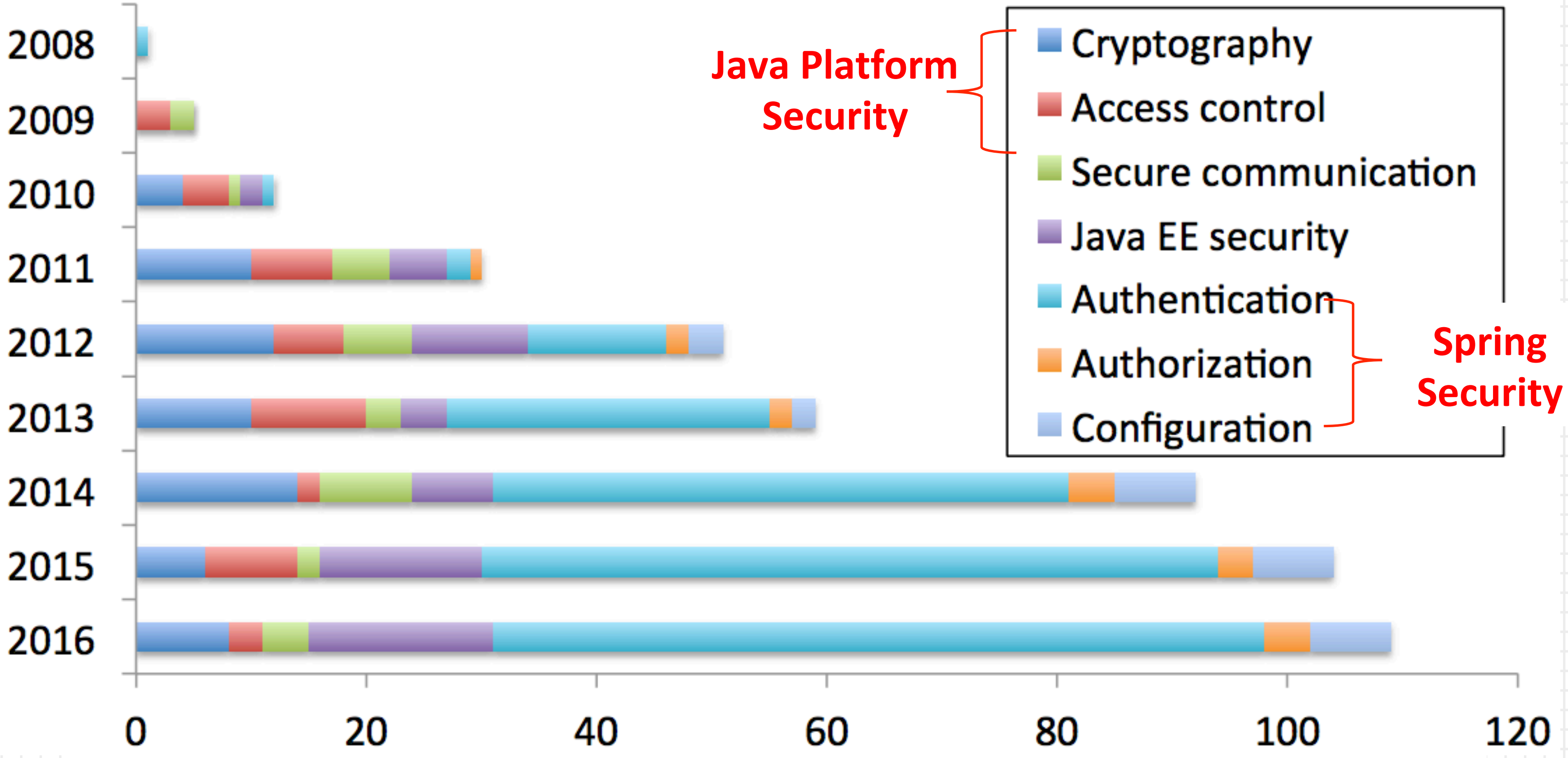
Other (2)

Configuration (26)

Authorization (16)

Authentication (225)

19% posts are about cryptography and SSL, indicating a lack of understand of the problem domain



Java Platform Security

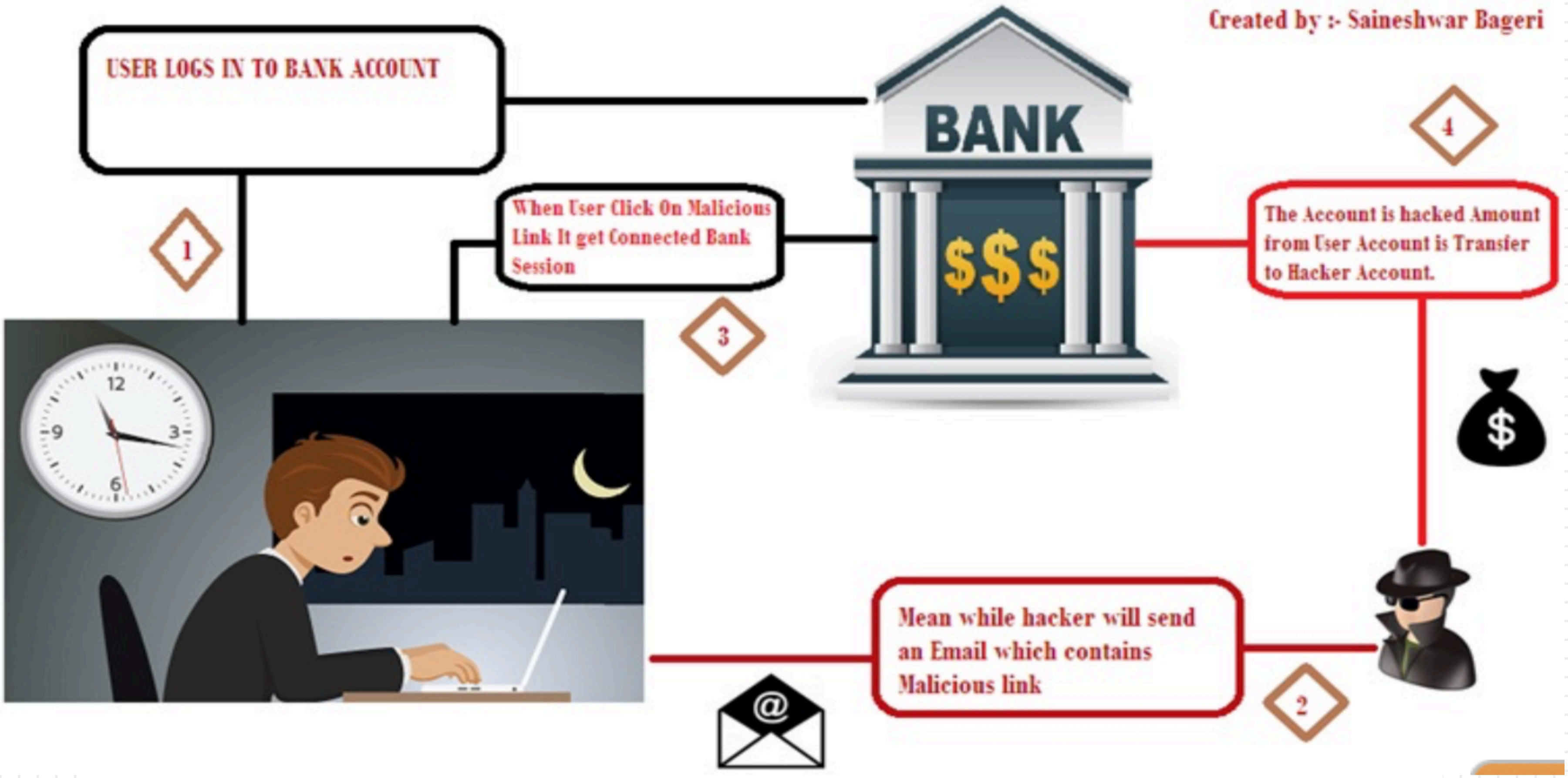
Spring Security

Developers’ major security concern has shifted from Java platform security to enterprise application security over the years.

RQ2: What are the common programming challenges?

- Authentication (for Spring Security)
  - Challenge 1: The way to integrate Spring Security with different applications varies a lot
    - E.g., Spring Boot, JBoss
  - Challenge 2: The two ways of security configuration (XML-based and Java-based) are hard to implement correctly
  - Challenge 3: Converting from XML-based to Java-based configuration is challenging

RQ3: What are the common securitv vulnerabilities?


Created by :- Saineshwar Bageri
USER LOGS IN TO BANK ACCOUNT
1
BANK
$$$
When User Click On Malicious Link It get Connected Bank Session
3
4
The Account is hacked Amount from User Account is Transfer to Hacker Account.
$
12
9
3
6
@
Mean while hacker will send an Email which contains Malicious link
2

https://www.acunetix.com/websitesecurity/csrf-attacks/

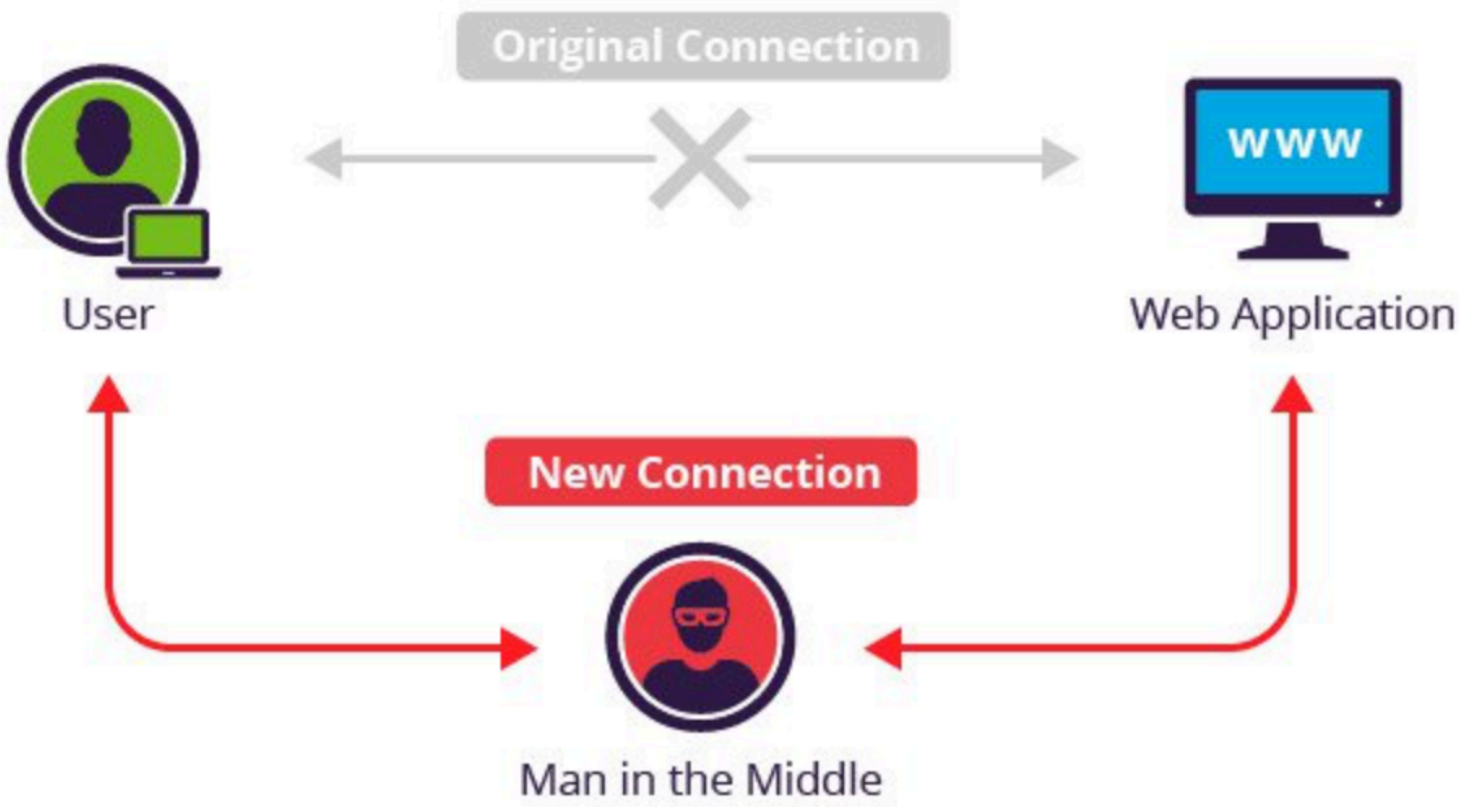
https://tedu.com.vn/bao-mat/series-bao-mat-trong-aspnet-mvc-2-cross-site-request-forgery-csrf-96.html?fb_comment_id=1813702025323664_1893585784001954#f22e0767c1eafae

SSL

```
//Create a trust manager that does not validate
certificate chains
TrustManager[] trustAllCerts = new TrustManager[] {
    new X509TrustManager() {
        public Java.security.cert.X509Certificate[]
            getAcceptedIssuers() { return null;}
        public void checkServerTrusted(…) {}   …
```

- Standard security technology for establishing an encrypted connection between a client browser and a webserver (HTTPS)
- TrustManager should be implemented to validate servers' certificates on the client side

Man-in-the-Middle (MITM) Attack



https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

9 of 11 SSL-relevant posts discussed insecure code

3 posts after 2012 discussed the dangerous solution

SO contains many obsolete and insecure practices

Social Aspects of Insecure Code on SO

Insecure Posts	Total Views	No. of Posts	Min Views	Max Views	Average
Disabling CSRF Protection*	39,863	5	261	28,183	7,258
Trust All Certs	491,567	9	95	391,464	58,594
Obsolete Hash	91,492	3	1,897	86,070	30,497
Total Views	**622,922**	**17**	-	-	-

Social Dynamics on SO

User: skanga
[0]

User: MarsAtomic
[6,287]

“Do NOT EVER trust all certificates. That is very dangerous.”

“the "accepted answer" is wrong and INDEED it is DANGEROUS. Others who blindly copy that code should know this.”

“once you have sufficient reputation you will be able to comment”

“If you don't have enough rep to comment, … then participate … until you have enough rep.”

https://stackoverflow.com/questions/10594000/when-i-try-to-convert-a-string-with-certificate-exception-is-raised

Conclusion

- A lot of developers do not appear to understand the security implications of coding options, showing a lack of cybersecurity training
- Spring Security usage is very popular, overly complicated, and poorly documented
- The social dynamics among askers and responders may impact people's security choices

Our StackOverflow data set is available at

http://people.cs.vt.edu/nm8247/icse18.xlsx

September 30-October 2, 2018 At the Hyatt Regency, Cambridge, MA

IEEE Secure Development Conference

Sponsored by the IEEE Cybersecurity Initiative and the IEEE Computer Society Technical Committee on Security and Privacy

Daphne Yao (VT)

Stephen Chong (Harvard)

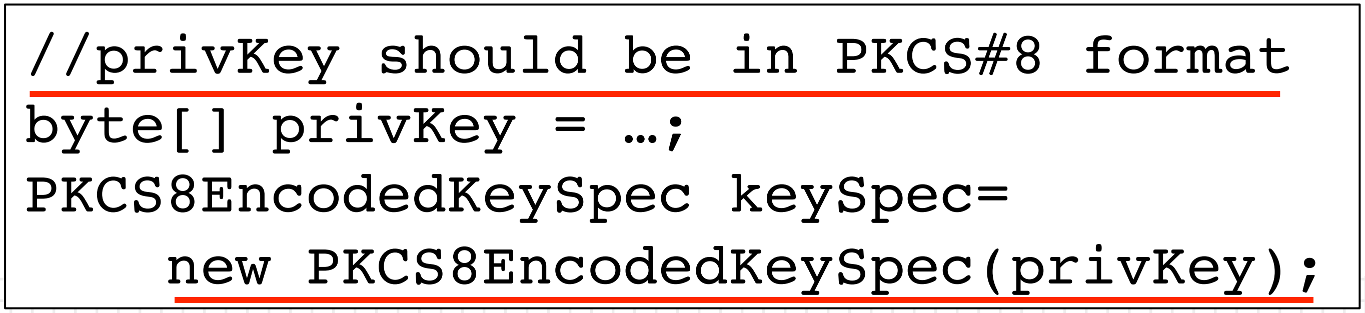
Submission open for 1-page abstracts

Practitioner’s abstract due: **July 20**

https://secdev.ieee.org/2018/home

References

- [Lazar et al. 2014] D. Lazar, H. Chen, X. Wang, and N. Zeldovich. Why does cryptographic software fail? A case study and open problems. APSys ’14.
- [Nadi et al. 2016] S. Nadi, S. Krüger, M. Mezini, and E. Bodden. Jumping through hoops: why do Java developers struggle with cryptography APIs? ICSE ’16.
- [Fahl et al. 2012] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, and M. Smith. Why Eve and Mallory love Android: An analysis of Android SSL (in)security. CCS ’12.
- [Georgiev et al. 2012] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov. The most dangerous code in the world: Validating SSL certificates in non-browser software. CCS ’12.
- [Acar et al. 2016] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky. You get where you’re looking for: The impact of information sources on code security. SP ’16.



```
//privKey should be in PKCS#8 format
byte[] privKey = …;
PKCS8EncodedKeySpec keySpec=
    new PKCS8EncodedKeySpec(privKey);
```

- Cryptography
  - Challenge 1: The error message did not provide sufficient useful hints about fixes
  - Challenge 2: It is difficult to implement security with multiple programming languages
    - E.g., Encryption in Python and decryption in Java
  - Challenge 3: Implicit constraints on API usage cause confusion

Research Questions

- What are the developers' common concerns on Java secure coding?
- What are the common programming challenges?
- What are the common security vulnerabilities?

SO Post Filtering

- Filter less useful posts
  - Removing duplicated posts, posts without accepted answers, and posts whose questions received negative votes
  - Removing posts without code snippets with keyword-based search: “public” and “class”
  - Discarding irrelevant posts based on manual inspection