Side-Channel Attacks on Web Applications

Cryptography Group, Department of Computer Science, University of Bristol

Web applications for online banking, tax declarations and health assessments (e.g. NHS direct) are complex, interactive programs, with more and more computation being moved from the client to a server (“into the cloud”). As a result, an increasingly large amount of our personal information is being transferred across the Internet.

To keep this information private, the Transport Layer Security (TLS) protocol using HTTP Secure (HTTPS) is deployed to encrypt our data as it travels between our personal computers and web application servers. However, recent research has shown that despite the use of these strong encryption schemes, our personal information can still be recovered by an attacker using side-channel information such as the size of encrypted network packets.

As a result, the secrecy of such personal data as financial status, medical condition and Internet search history is threatened.

Motivation
Web applications for online banking, tax declarations and health assessments (e.g. NHS direct) are complex, interactive programs, with more and more computation being moved from the client to a server (“into the cloud”). As a result, an increasingly large amount of our personal information is being transferred across the Internet.

To keep this information private, the Transport Layer Security (TLS) protocol using HTTP Secure (HTTPS) is deployed to encrypt our data as it travels between our personal computers and web application servers. However, recent research has shown that despite the use of these strong encryption schemes, our personal information can still be recovered by an attacker using side-channel information such as the size of encrypted network packets.

As a result, the secrecy of such personal data as financial status, medical condition and Internet search history is threatened.

Disclosure of medical information

The value we place on the secrecy of our personal information is high, and so the development of tools that can detect situations where a web application ‘leaks’ our private data is critical.

Previous work on tools for solving this problem with web applications has mostly drawn from techniques used in the field of machine learning, and therefore has not tapped into the substantial body of knowledge that has been generated in the course of detecting and exploiting leaks from physical cryptographic devices.

Having contributed ourselves to this existing body of knowledge we recognised the need to first concentrate on devising a reliable and flexible leakage detection test for web applications. Our new test can recognise leaks from a variety of sources and can be extended to incorporate multiple sources within a single test. Whilst research into this ‘new’ application of side-channel attacks has just begun, its potential and importance for the wider society is significant.

With government initiatives driving the development of electronic health systems and the continuing trend towards the outsourcing of private information, the development of robust implementations of web applications that by design attempt to minimise the leakage of our data is imperative.

Our future work will concentrate on the analysis of this problem, with the goal of aiding in the design and development of robust and efficient defences against these attacks.

Contribution and Outlook
The value we place on the secrecy of our personal information is high, and so the development of tools that can detect situations where a web application ‘leaks’ our private data is critical.

Previous work on tools for solving this problem with web applications has mostly drawn from techniques used in the field of machine learning, and therefore has not tapped into the substantial body of knowledge that has been generated in the course of detecting and exploiting leaks from physical cryptographic devices.

Having contributed ourselves to this existing body of knowledge we recognised the need to first concentrate on devising a reliable and flexible leakage detection test for web applications. Our new test can recognise leaks from a variety of sources and can be extended to incorporate multiple sources within a single test. Whilst research into this ‘new’ application of side-channel attacks has just begun, its potential and importance for the wider society is significant.

With government initiatives driving the development of electronic health systems and the continuing trend towards the outsourcing of private information, the development of robust implementations of web applications that by design attempt to minimise the leakage of our data is imperative.

Our future work will concentrate on the analysis of this problem, with the goal of aiding in the design and development of robust and efficient defences against these attacks.

Funding and Collaboration

EPSRC via grant EP/I005226/1
European Commission via ECRYPT II