CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Integrating Privacy Practices into the Software Development Life Cycle

Key Message: Addressing privacy during software development is just as important as addressing security.

Executive Summary

Clearly security and privacy are closely linked when it comes to protecting information, yet when it comes to software development, privacy hasn't yet pulled the same profile as security. As is the case for security, privacy is most effectively addressed when privacy practices, roles, responsibilities, and review approvals are integrated into your existing software and security development lifecycle. This helps ensure that privacy is at the forefront of developers' minds as they execute each lifecycle phase.

In this podcast, Ralph Hood and Kim Howell, both with Microsoft's Trustworthy Computing Initiative, will discuss Microsoft's top ten privacy practices and how they have been integrated with their security development lifecycle (SDL). Ralph is a lead program manager on the SDL team and Kim is a director in the Privacy group.

PART 1: KEEPING PRIVACY AT THE FOREFRONT; COLLECT ONLY ESSENTIAL INFORMATION

Addressing Privacy during Software Development

As is the case for security, it is important for developers to keep privacy at the forefront of their thinking, addressing it as early in the lifecycle as possible.

Key topics include

- identifying privacy contacts
- performing an initial privacy assessment
- defining the project's
- designing for privacy
- ensuring valid test cases for privacy scenarios

Integrating privacy practices with security practices and with the software development lifecycle helps minimize the overhead for developers, giving them a single process where this is all defined.

Security and privacy practices address the obligations that a company takes on when they collect and use personal data.

Defining User and Personal Data

First, organizations need to protect Personally Identifiable Information (PII) – anything that would allow you to identify, contact, or locate an individual.

It is also important to protect pseudonymous information – anything collected about a user that would allow you to directly, inferentially, or implicitly derive an identity. The more you collect, the more you can infer.

Key Questions Developers Should Ask

When it comes to collecting user data, developers should always ask "Why am I collecting this data? Is it essential to provide the service I am developing?"

Every time you collect information, you create an obligation to maintain the security of that information for its life span. Having the potential for future use of the information may not be a sufficiently compelling reason for collecting it.

PART 2: MINIMIZE COLLECTED DATA; PREVENT UNAUTHORIZED ACCESS

Minimizing the Collection of Personal Data

According to Microsoft’s “Ten Things You Must Do to Protect Privacy,” (see Resources), minimizing the collection of personal data includes the following practices:

- Collect user data only if you have a compelling business and user value proposition.
- Collect the smallest amount of data for the shortest period of time.
- Collect the least sensitive form of data.

Make sure that you map data collection to a business need. You need to understand not only what data you are collecting but its context and associations. For example, if personal data is going to be aggregated, you don’t need to collect PII. If you do collect PII, you need to discard it as soon as possible.

It is important to hold data for the shortest period of time. This can be tackled, for example, by automating the time duration for retaining log files and data that is extracted from log files.

Preventing Unauthorized Access and Inappropriate Use

According to Microsoft’s “Ten Things You Must Do to Protect Privacy,” the following practices should be considered in order to prevent unauthorized access and inappropriate use of personal data:

- Prevent unauthorized access to personal data.
- Provide administrators with a way to prevent transfers.
- Honor the terms that were in place when the data was originally collected.

What constitutes unauthorized access is defined by the level of notice and consent you receive from the user at the time of collection. You must make sure privacy preferences, sources, contact preferences, etc. travel with and stay associated with the user data that you collect in order to insure that during development, only authorized access is permitted.

You need to provide system administrators with the right tools so that they can define and implement their appropriate use policies.

Interacting with Users about Their Data

According to Microsoft’s “Ten Things You Must Do to Protect Privacy,” interacting with users about their data includes the following practices:

- Provide a prominent notice and obtain explicit consent before transferring personal data from the user's computer.
- Get parental consent before collecting and transferring a child's personal data.
- Provide users access to their stored personal data.
- Respond promptly to user questions about privacy.

You need to consider the type of data you’re collecting and your purpose in collecting it.

You can

- provide notice in a discoverable privacy statement
- give notice right in the user interface for more privacy-invasive data. This is called “unavoidable.”
- provide tools where users can change their settings

PART 3: GAIN PARENTAL CONSENT; ENSURE PRIVACY IN THE SDL

Gaining Parental Consent

You need to determine if what you are developing either directly targets or may be attractive to children. Both of these conditions create some obligations when collecting PII.

The U.S. Child Online Protection Act (COPA) is a law that addresses collecting data from minors. Knowingly collecting such information requires parental consent.

Addressing Privacy in the Security Development Lifecycle

The SDL also kicks off a privacy review process. Privacy managers work with development teams starting early on in the design process.

Privacy managers

- review the initial design
- help to minimize privacy issues
- help define the right notice and consent experiences for data collection
- conduct a final privacy review, approval, and signoff

No products ship without a privacy signoff.

An increasing number of organizations are starting to use Microsoft’s privacy guidelines.

Resources

Microsoft’s Security Development Lifecycle web site

Microsoft Security Development Lifecycle (SDL) – Version 4.1a, November 6, 2009. Appendix A – Privacy at a Glance summarizes “Ten Things You Must Do to Protect Privacy.”

Microsoft’s SDL blog

Microsoft’s Privacy web site

Microsoft’s Privacy Guidelines for Developing Software Products and Services, Version 3.1, September 2008.