2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Survey response	FY 2016	FY 2015
Total sampling frame	8,680	8,891
Total returns	590	595
Rejected or screened surveys	63	71
Final sample	527	524
Response rate	6.1%	5.9%

Part 1. Screening questions

S1. What best describes your role?	FY 2016	FY 2015
Software engineer	21%	18%
Software designer	12%	14%
Software developer	22%	20%
Software programmer	15%	17%
Supervisor of software development	8%	9%
Manager of software development	9%	10%
IT security	6%	7%
Corporate IT	7%	6%
None of the above (stop)	0%	0%
Total	100%	100%

S2. What best describes your company's role in the automotive industry?	FY 2016	FY 2015
Manufacturer OEM	44%	45%
Tier One	29%	31%
Tier Two	21%	19%
Tier Three	6%	5%
None of the above (stop)	0%	0%
Total	100%	100%

S3. How familiar are you with your company's program to secure software for automobiles?	FY 2016	FY 2015
Very familiar	33%	29%
Familiar	48%	51%
Somewhat familiar	19%	20%
No knowledge (stop)	0%	0%
Total	100%	100%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Part 2. Attributions: Please rate each one of the following statements using the scale provided below each item.

Q1a. My company makes automotive security a priority.	FY 2016	FY 2015
Strongly agree	16%	14%
Agree	31%	27%
Unsure	30%	30%
Disagree	16%	20%
Strongly disagree	7%	8%
Total	100%	100%

Q1b. My organization recruits and retains expert personnel to minimize security risks in automobiles.	FY 2016	FY 2015
Strongly agree	17%	16%
Agree	34%	29%
Unsure	26%	29%
Disagree	17%	19%
Strongly disagree	6%	7%
Total	100%	100%

Q1c. Automotive development teams have the skills necessary to combat cybersecurity threats.	FY 2016	FY 2015
Strongly agree	15%	16%
Agree	32%	27%
Unsure	27%	30%
Disagree	20%	20%
Strongly disagree	6%	7%
Total	100%	100%

Q1d. Hackers are actively targeting automobiles.	FY 2016	FY 2015
Strongly agree	20%	15%
Agree	32%	29%
Unsure	28%	31%
Disagree	16%	18%
Strongly disagree	4%	7%
Total	100%	100%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Q1e. Automakers are not as knowledgeable about secure platform development as other industries are.	FY 2016	FY 2015
Strongly agree	14%	17%
Agree	25%	27%
Unsure	29%	28%
Disagree	23%	20%
Strongly disagree	9%	8%
Total	100%	100%

Q1f. My company's automotive development process includes activities for security requirements, design, implementation and testing.	FY 2016	FY 2015
Strongly agree	16%	15%
Agree	31%	27%
Unsure	24%	29%
Disagree	20%	21%
Strongly disagree	9%	8%
Total	100%	100%

Q1g. Engineers and developers are adequately trained in secure architecture and coding practices.	FY 2016	FY 2015
Strongly agree	20%	18%
Agree	29%	27%
Unsure	28%	30%
Disagree	16%	18%
Strongly disagree	7%	7%
Total	100%	100%

Q1h. It will be the norm for my company to participate in open disclosure of bugs and bug bounty programs.	FY 2016	FY 2015
Strongly agree	17%	18%
Agree	26%	27%
Unsure	28%	30%
Disagree	22%	18%
Strongly disagree	7%	6%
Total	100%	100%

Q1i. My company has the enabling technologies to ensure automotive development is secure.	FY 2016	FY 2015
Strongly agree	19	17%
Agree	27	29%
Unsure	30	29%
Disagree	16	19%
Strongly disagree	8	7%
Total	100	100%

Sponsored by Security Innovation and Integrity Security Services

Ponemon Institute

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Part 3. Background Questions

Q2a. Who is the person **most** responsible and accountable for security in your automotive development process?	FY 2016	FY 2015
Developers	12%	11%
Quality Assurance	18%	21%
Chief Information Security Officer	17%	19%
Chief Information Officer	22%	24%
Partners	11%	
Other	1%	2%
No one	19%	
Total	100%	

Q2b. Who is most responsible and accountable for security of digital trust assets (i.e. intellectual property, cryptographic keys, etc.) in your manufacturing process?	FY 2016
Developers	4%
Quality Assurance	5%
Chief Information Security Officer	21%
Chief Information Officer	36%
Partners	13%
Other	3%
No one	18%
Total	100%

Q3. What are the main challenges to securing automobile software? Please select the top three challenges.	FY 2016	FY 2015
Lack of skilled personnel	65%	67%
Insufficient resources	58%	64%
Pressure to release	65%	54%
Lack of defined corporate application security policies	43%	48%
Lack of formal security requirements	34%	38%
Too expensive	11%	
Adds too much time to the software development process	18%	16%
Other	6%	12%
Total	300%	300%

Q4. What percentage of the total time to develop software is spent testing its security?	FY 2016	FY 2015
Less than 2%	20%	25%
2 to 5%	19%	22%
6 to 10%	16%	12%
11 to 15%	11%	9%
16 to 20%	11%	10%
21 to 25%	7%	8%
26 to 30%	8%	8%
31 to 40%	6%	5%
More than 40%	2%	1%
Total	100%	100%
Extrapolated value	12.5%	11.3%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Q5a. Is security a priority for your company?	FY 2016	FY 2015
Yes	54%	49%
No	46%	51%
Total	100%	100%

Q5b. If no, why? Please select your top two reasons.	FY 2016	FY 2015
Lack of expertise	12%	10%
Takes too much time	20%	22%
Pressure to complete development	29%	24%
Additional costs to secure software	22%	19%
Not considered important	16%	22%
Other	1%	3%
Total	100%	100%

Q6. What methods does your team use to ensure code is secure without vulnerabilities? Please select all that apply.	FY 2016	FY 2015
Automated scanning tools to test applications during development	65%	63%
Automated scanning tools to test applications in production	25%	22%
Automated scanning tools to test applications for vulnerabilities after they have been released	48%	50%
Manual penetration testing by internal teams or a third party	41%	36%
Adherence to secure coding standards	23%	25%
Threat model or other high-level risk assessment process is followed during the development process	24%	24%
Other	3%	10%
None of the above	27%	
Total	256%	230%

Q7. What security issues worry you most? Please select only one choice.	FY 2016	FY 2015
IP protection	31%	
Safety of vehicles	39%	36%
Increased government regulations	15%	
Data privacy	12%	
Other	3%	4%
Total	100%	

Sponsored by Security Innovation and Integrity Security Services

Ponemon Institute

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Part 4. Secure software practices in the automotive industry

Q8. How difficult is it to secure automobiles? Please use the following scale from 1 = Not difficult to 10 = Very difficult.	FY 2016	FY 2015
1 to 2	1%	2%
3 to 4	7%	9%
5 to 6	18%	21%
7 to 8	39%	33%
9 to 10	35%	36%
Total	100%	100%
Extrapolated value	7.50	7.40

Q9. Do you believe legacy technology, such as CAN and OBD-II, is hindering the industry from making vehicles more secure?	FY 2016
Yes	55%
No	40%
Unsure	5%
Total	100%

Q10. Should OEMs be liable for security vulnerabilities in their suppliers' designs?	FY 2016
Yes	44%
No	49%
Unsure	7%
Total	100%

Q11a. Does your company include cryptography as part of its secure software development?	FY 2016
Yes	46%
No	50%
Unsure	4%
Total	100%

Q11b. If cryptography is not used, why?	FY 2016
Lack of knowledge	25%
Too expensive	21%
No explicit requirement	33%
Better alternatives available	13%
Unsure	6%
Other	2%
Total	100%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Q12. Is it possible to build an automobile that is nearly hack proof?	FY 2016	FY 2015
Yes	17%	19%
No	55%	47%
Unsure	28%	34%
Total	100%	100%

Q13a. Does your company integrate security architecture design into the development process or is it an add-on?	FY 2016	FY 2015
Totally integrated	15%	14%
Partially integrated	34%	29%
Added on	47%	51%
Unsure	4%	7%
Total	100%	100%

Q13b. Does your company integrate the security architecture, including the entire supply chain and partner network?	FY 2016
Totally integrated	11%
Partially integrated	29%
Added on	55%
Unsure	5%
Total	100%

Q14. Which of the following system security features does your company currently use? Select all that apply	FY 2016
Secure boot	53%
Encrypted communication	44%
Endpoint authentication	39%
Encrypted data in storage	42%
Other	6%
Total	184%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Q15. What security hardware features are required in your processor selection?	FY 2016
Cryptographic Acceleration	21%
Protected Key Storage	43%
True Random Number Generation	32%
Hypervisor Memory Management Support	27%
Other	6%
None of the above	40%
Total	169%

Q16. Should cars include event-logging equipment to better understand when an attack has taken place?	FY 2016	FY 2015
Yes, event-logging equipment should be in cars	21%	18%
Yes, but only as an option	42%	38%
No	34%	40%
Unsure	3%	4%
Total	100%	100%

Q17. Should software updates be handled by Over-the-Air (OTA) updates or in controlled environments such as factories or dealerships?	FY 2016	FY 2015
Yes, updates should be handled by OTA	35%	30%
No, software updates should only be handled in controlled environments such as factories or dealerships	35%	35%
Unsure	30%	36%
Total	100%	100%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

Part 5. Your role and organization

D1. What organizational level best describes your current position?	FY 2016	FY 2015
Senior Executive/VP	3%	4%
Director	17%	18%
Manager	20%	17%
Supervisor	15%	17%
Technician/Staff	39%	38%
Consultant/Contractor	6%	5%
Other	0%	1%
Total	100%	100%

D2. Check the primary person you or your leader (direct supervisor) reports to within the organization.	FY 2016
Head, Application Development	34%
Head, Quality Assurance	14%
Chief Information Officer	21%
Chief Technology Officer	9%
Chief Information Security Officer	9%
Compliance Officer	0%
Chief Security Officer	1%
Data Center Management	2%
Chief Risk Officer	3%
Other	7%
Total	100%

2016 Application Security Practices in the Automotive Industry

Audited findings presented by Ponemon Institute

D3. In which areas of development are you involved? (Check all that apply)	FY 2016
Software design/development/test	54%
Hardware selection/implementation	25%
Cryptography selection/implementation	29%
Operating system selection/implementation	25%
Management	40%
Other	6%
Total	179%

D4. What is the worldwide headcount of your organization?	FY 2016	FY 2015
Less than 100	4%	5%
100 to 500	14%	13%
501 to 1,000	10%	12%
1,001 to 5,000	10%	11%
5,001 to 10,000	12%	10%
10,001 to 25,000	17%	15%
25,001 to 75,000	13%	15%
More than 75,000	20%	19%
Total	100%	100%

D5. How many software developers work in your organization?	FY 2016	FY 2015
I am an independent software developer (freelancer)	9%	10%
Less than 100	12%	13%
101 to 1,000	15%	16%
1,001 to 5,000	27%	25%
5,001 to 10,000	29%	28%
More than 10,000	8%	7%
Total	100%	100%

D6. Where are your employees located? (Check all that apply):	FY 2016	FY 2015
United States	100%	100%
Canada	97%	100%
Europe	72%	70%
Asia-Pacific	60%	58%
Middle East & Africa	39%	41%
Latin America (including Mexico)	37%	31%
Total	405%	399%